

**CISA Tabletop Exercise Package Healthcare and Public Health Sector**

## [Enter Organization Name]

## <Insert Date>

Updated October 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 11](#_Toc143606191)

[Appendix A: Additional Discussion Questions 14](#_Toc143606192)

[Appendix B: Acronyms 17](#_Toc143606193)

[Appendix C: Case Studies 18](#_Toc143606194)

[Appendix D: Attacks and Threats 19](#_Toc143606195)

[Appendix E: Contacts and Resources 21](#_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 | Examine the cyber resilience of <Organization> in response to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess the cyber resilience of <Organization> during and following a cyber incident impacting network connected medical devices. 2. Evaluate the impacts of a cyber incident on patient care and operations. 3. Improve IT and OT cybersecurity coordination to enhance the cybersecurity posture of <Organization>. 4. Evaluate <Organization’s> ability to restore operations after disruptions from cyber intrusions. | |
| Threat or Hazard | Phishing, Ransomware | |
| Scenario | A threat actor targets employees through phishing emails. Imaging equipment, patient records, and other medical equipment begin malfunctioning/displaying incorrect data. Personal Health Information (PHI) data is exfiltrated, and ransomware compromises computer systems and equipment. | |
| 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 presented in this scenario.
* Appendix D: An explanation of the threats presented in this scenario.
* Appendix E: Additional cybersecurity preparedness and response resources.

## Participant Roles and Responsibilities

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

**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 several events, including a suspicious email to employees and an unannounced vendor.
  + **Module 2:** This module includes a ransomware attack and the discovery of patient data theft.
* Hotwash
* ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

## Exercise Guidelines

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

## Exercise Hotwash and Evaluation

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

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA), the Federal Bureau of Investigation (FBI), and the Department of Health and Human Services (HHS) Health Sector Cybersecurity Coordination Center (HC3) release a joint alert regarding a rise in cyberattacks targeting healthcare organizations. The alert describes the tactics, techniques, and procedures (TTPs) used by cyber criminals, including phishing emails, ransomware, remote hacking, distributed denial of service (DDoS) attacks, and data exfiltration from healthcare organizations.[[2]](#footnote-3)

### Day 9

<Organization> employees receive e-mail notifications from your managed service provider (MSP) requesting they update their profiles prior to the launch of a new human resources (HR) system.[[3]](#footnote-4) The e-mail contains a link and attachment named *Update\_Form.docx*. Employees working at remote workstations across facilities click the link and are asked to log into their web portal. Upon logging in, they are brought to a 404 Error Page. Some employees also open the attachment and click to allow macros to run.

## Discussion Questions

Discussion questions included throughout 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 (e.g., information from CISA, Health-ISAC, HHS)?
3. What cyber threat information is most useful?
4. How is information disseminated throughout your organization and by whom?
5. What actions would your organization take in response to an alert like the one presented in the scenario?
6. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
   1. What information technology (IT) systems or processes are the most critical to your organization?
   2. Describe your organization’s asset management plan and how you prioritize critical assets.
   3. What improvements have been implemented to enhance cyber resilience following recent risk assessments?
   4. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
7. 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. What type of training methods or approaches have you found most beneficial?
8. How are employees trained to recognize and report cyber threats such as phishing scams?
   1. What additional training does your organization require for those who fall for a fake phishing campaign?
9. How do users report suspicious emails?
   1. What procedures or plans would be followed once a suspicious email has been reported?
10. Describe your organization’s cybersecurity posture.
    1. How frequently are users required to change their passwords?
    2. Does your organization use multi-factor authentication (e.g., something you know, something you have, something you are) to mitigate the potential effects of phishing?
11. What are your network access and authentication controls for users?[[4]](#footnote-5)
    1. Does your organization allow users to run document macros? If so, what compensating security controls do you have to mitigate the risk?
    2. What cybersecurity controls are present to mitigate the risk of users entering credentials into phishing websites?

### Day 10

Manufacturer’s updates are pushed for installation on patient monitors. The updates are downloaded from the manufacturer’s website and installed without issue.[[5]](#footnote-6)

### Day 13

A third-party electronic medical record (EMR) vendor shows up unannounced at your facility to update equipment. The vendor needs to patch a recently discovered vulnerability in software used on several devices, including workstations, imaging and radiology equipment, bedside monitors, and other clinical devices.[[6]](#footnote-7)

1. What cybersecurity language is included within third-party vendor contracts?
2. How do you evaluate the cybersecurity posture of your vendors?
3. How often are contracts reviewed?
4. How do your service level agreements address cyber incident notification?
5. How do vendors notify you that patches or updates are required?

### Day 15

Radiology reports an issue with their Magnetic Resonance Imaging (MRI) machine accepting patient information, stating their computer is locking up or taking a long time to load. The reports also indicate an extraordinary amount of time is required to pull images for each patient. The delays have resulted in patient appointments running more than two hours behind schedule.[[7]](#footnote-8)

1. Describe your organization’s software patch management plan and patching procedures.[[8]](#footnote-9)
   1. What processes are used to evaluate and maintain an approved list of patches?
   2. How does risk inform decisions regarding allowed hardware, firmware, and software updates?
   3. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?
2. What level of access do your third-party vendors have to your organization’s network?

# Module 2

### Day 20

A system administrator discovers active accounts for IT employees that left the organization over the past 12 months. The administrator closes them out.[[9]](#footnote-10)

### Day 23 - Morning

Nurses on the floor report that patient records are displaying incorrect information about medication, diagnosis, and personal information.[[10]](#footnote-11)

### Day 23 - Afternoon

Staff discover bedside monitor data is inaccurate and the infusion pumps are not operating properly and are failing to deliver infusions at the correct rate.[[11]](#footnote-12)

## Discussion Questions

1. Using your organization’s existing incident response plan/cyber incident response plan (CIRP), describe the actions your organization would take at this time.
2. Describe the training your employees receive on this plan.
3. What guidance does the plan include on assessing the severity of the incident?
4. How does incident severity level dictate response?[[12]](#footnote-13)
5. How are critical systems and processes incorporated within your CIRP?
6. Does your organization have backups of vital records and EMRs stored in a location separate from your primary working files/copies?
7. How frequently do you run backups?
8. How long do you keep copies of archived files backed up?
9. How long would it take to restore primary files from backups?
10. What redundant systems exist for when primary systems are compromised?
11. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
12. Who can authorize use of alternate systems or procedures?
13. How long can you perform manual or alternate processes on your critical systems?
14. What additional resources are required to operate with manual processes?

### Day 25

Ransomware messages appear on computers throughout <organization>, and users report they are unable to access their files.[[13]](#footnote-14) A message is displayed that reads:

“Hello! Your files have been liberated. We have your data. But do not fear because for the sum of $1,000,000 your files will be returned. The decryption key will expire in 72 hours. Please submit payment to the wallet below or we will start selling patient data to the highest bidder.”

### Day 26

Current and former patients contact the hospital saying they received calls from someone claiming to have access to their medical records and offering to return them for a fee. The patients are provided enough information to verify the callers have their records.

Patients say the fees range from a few hundred dollars to more than a thousand and are demanding to know why these individuals have their records.

Some say they contacted law enforcement; others contacted the media. Many are threatening legal action.

### Day 27

Patients request transfers to other local hospitals because they feel unsafe. They also demand the return of all their medical records, as well as the removal of their records from your network. The patients state they will never return your facilities.[[14]](#footnote-15)

1. Using your CIRP as a guide, how have your priorities changed based on these recent events?
2. Explain your organization’s decision-making process regarding ransomware payment.[[15]](#footnote-16)
3. Are ransomware policies/procedures included in your CIRP?
4. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
5. Discuss the advantages and disadvantages of either agreeing or refusing to pay the ransom.
6. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
7. Describe the impact the sale or release of sensitive information or PHI would have on your response and recovery activities.
8. What security breach notification laws does your state or industry have?
9. Describe your organizational processes to respond to the media reports and inquiries.
10. What pre-scripted messages have been developed for cyber incidents?
11. How would public messaging be coordinated and disseminated during a cyber incident?
12. How would you preserve and reinforce the public’s confidence and trust in your organization during a significant cyber incident?
13. Based on discussion, what changes would 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. Exercise planners are encouraged to select additional, applicable discussion questions for the chosen scenario to bolster participant conversation. *This instructional page, as well as undesired discussion questions, should be deleted.*

## Cyber Resilience

1. How does your organization integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
2. Describe your organization’s review process for your CIRP.
3. How often is the CIRP reviewed?
4. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
5. How are updates to the plan communicated to department or agency employees?
6. How does your organization mitigate insider threats?
   1. Does your organization have an insider threat management program?
   2. What type of training do employees at your organization receive on identifying a potential insider threat?
7. Discuss your supply chain concerns related to cybersecurity infrastructure.
8. What level of access do your third-party vendors have to your organization’s network?
9. How does your organization baseline network activity?
   1. How does your organization distinguish between normal and abnormal traffic?
10. What is your method for tracking and identifying firmware vulnerabilities in your organization’s network?
11. How would the scenario events affect your organization’s business operations/processes?
12. How is the integrity of your critical data protected and validated?
13. How would those entities report a breach of their systems to your office?
14. What is your cyber incident management structure?
15. Who leads incident management and why?
16. How are they notified?
17. How often are roles and responsibilities within this structure exercised with employees?
18. What essential functions are impacted by the incidents described in the scenario?
19. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
20. What mechanisms (e.g., Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA), contract, etc.) are in place for arranging additional surge support of both personnel and resources if needed?
21. If primary communications are compromised, how do you provide information to internal and external entities?
22. 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?

## Employee Accounts and Privileges

1. How regularly are users required to change their passwords?
   1. What is your organization’s account lockout policy if users do not change their passwords in a timely fashion?
   2. What are your organization’s requirements for password length and level of complexity?
2. Describe your organization’s employee off-boarding process.
3. Is this process coordinated with Information Technology (IT) and Human Resources (HR)?
4. What additional actions are taken if the employee’s termination is contentious?
5. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication key, system administration's handbook/manual, keys, identification cards, etc.)?
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?

## 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 cyber incident response plan?
4. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
5. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
6. How often is your organization’s data reviewed?
   1. 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. What are the roles of your network operations center and security operations center during a response?
5. What are the processes for contacting critical personnel outside of core hours?
6. How do you proceed if critical personnel are unreachable or unavailable?

## 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 would the process be to completely rebuild these systems?
7. What factors do you consider when making these decisions?

## Training and Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
2. How often does your organization exercise its CIRP?
3. How does your organization’s training and exercise efforts address both physical and cyber risks?
4. 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?
2. How do these goals align with organizational objectives?
3. What cybersecurity training is required for senior leadership?
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 information are you sharing internally (e.g., with employees, leadership)?
      2. What information are you sharing externally (e.g., with patients, vendors)?
      3. What training is provided to employees on reporting any contact with the media to the appropriate public information personnel?
      4. How do you build and maintain trust with your patients and the community?

## Legal

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

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| 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 |
| EHR | Electronic Health Record |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| HHS | U.S. Department of Health and Human Services |
| IT | Information Technology |
| MRI | Magnetic Resonance Imaging |
| MSP | Managed Service Provider |
| NIST | National Institute of Standards and Technology |
| PHI | Protected Health Information |
| PII | Personally Identifiable Information |
| TLP | Traffic Light Protocol |

# Appendix C: Case Studies

## Ransomware Attack Against Healthcare System

On August 3, 2023, a healthcare system that operates 16 hospitals and more than 160 clinics and outpatient centers across four states, experienced a ransomware attack. The attack forced some locations to close and others to rely on paper records.[[16]](#footnote-17) One affiliate of the system indefinitely closed a medical imaging center, an urgent care facility, and an outpatient blood-draw center. Others had to close emergency rooms and divert ambulances to other facilities, delaying critical care to patients.[[17]](#footnote-18)

The healthcare system did not respond to the hackers’ ransom demands and on August 29, 2023, medical records extracted during the attack were found on the dark web. The hackers posted a timer with the following message: “With just 7 days on the clock, seize the opportunity to bid on exclusive, unique, and impressive data…more than 500,000 SSN, passports of [healthcare system] clients and employees, driver’s licenses, patient files (profiles and medical history), financial, and legal documents!”[[18]](#footnote-19)

## Data Breach Impacts 8.8 Million Americans

Between February 26, 2023, and March 7, 2023, one of the largest dental insurers of government-sponsored dental plans (Medicaid and CHIP) in the United States, fell victim to a data breach that impacted more than 8.8 million Americans. An unauthorized third party infected the victim’s network with malicious code and removed copies of personal and protected health information (PHI).[[19]](#footnote-20) The intruders gained access to and exfiltrated PHI such as full names, Social Security numbers, insurance information, and driver’s licenses or other government identification numbers.[[20]](#footnote-21) The LockBit ransomware group claimed responsibility for the attack and when the victim refused to pay the $10 million ransom, the group published the stolen files on April 7, 2023.

After the attack, the dental insurer enhanced their security controls to minimize the risk of future incidents. However, numerous impacted individuals filed lawsuits against the dental insurer, alleging the organization “knew or should have known that its patients’ personal information was a tempting target for cybercriminals, but failed to implement data security standards that were required under federal and state laws and industry standards.”[[21]](#footnote-22),[[22]](#footnote-23)

# Appendix D: Attacks and Threats

## Data Loss and Data Theft

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

### Additional Resources

* Protecting Sensitive and Personal Information (<https://www.cisa.gov/resources-tools/resources/protecting-sensitive-and-personal-information>)
* Cybersecurity and Physical Security Convergence Action Guide (<https://www.cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide>)

## Insider Threat

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

### Additional Resources

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

## 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 (<https://www.cisa.gov/stopransomware/healthcare-and-public-health-sector>)
* 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

* Phishing Guidance: Stopping the Attack Cycle at Phase One (<https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one>)
* Avoiding Social Engineering and Phishing Attacks (<https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks>)

## Healthcare and Public Health (HPH) Sector Threat and Mitigation Resources

* HHS 405(d) Managing Threats and Protecting Patients (<https://405d.hhs.gov/threats>)
* HHS Health Sector Cybersecurity Coordination Center (HC3) Threat Briefs and Sector Alerts: (<https://www.hhs.gov/about/agencies/asa/ocio/hc3/products/index.html#threat-briefs>)

# Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* 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)
* 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>)

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/>)

Healthcare and Public Health Sector Preparedness Resources

* Healthcare and Public Health Toolkit (<https://www.cisa.gov/topics/cybersecurity-best-practices/healthcare>)
* HHS Administration for Strategic Preparedness and Response (ASPR) Technical Resources, Assistance Center & Information Exchange (TRACIE) Resources
* Technical Resources Page (<https://asprtracie.hhs.gov/technical-resources>)
* Healthcare System Cybersecurity: Readiness and Response Considerations (<https://files.asprtracie.hhs.gov/documents/aspr-tracie-healthcare-system-cybersercurity-readiness-response.pdf>)
* Healthcare System Cybersecurity Response: Experiences and Considerations Webinar (<https://files.asprtracie.hhs.gov/documents/cybersecurity-response-experiences-and-considerations-webinar-final.pdf>)
* Critical Infrastructure Protection (CIP) Cybersecurity Weekly Bulletin Signup (<https://www.phe.gov/Preparedness/planning/cip/Pages/CIPInquiry.aspx>) (contact: [CIP@hhs.gov](mailto:CIP@hhs.gov))
* HHS Health Sector Cybersecurity Coordination Center (HC3) (<https://www.hhs.gov/about/agencies/asa/ocio/hc3/index.html>) (contact: [HC3@hhs.gov](mailto:HC3@hhs.gov))
* HHS 405(d): Aligning Healthcare Security Approaches (<https://405d.hhs.gov/information>) (contact: [Cisa405d@hhs.gov](mailto:Cisa405d@hhs.gov))
* HPH Cybersecurity Framework Implementation Guide (<https://aspr.hhs.gov/cip/hph-cybersecurity-framework-implementation-guide/Pages/default.aspx>)
* Healthcare Sector Coordinating Council (HSCC) Recommended Cybersecurity Practices (<https://healthsectorcouncil.org/hscc-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/))

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.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-4)
4. 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-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.PS-02: Software is maintained, replaced, and removed commensurate with risk,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-02>. [↑](#footnote-ref-7)
7. NIST CSF 2.0 via CPRT, “DE: Detect – Possible cybersecurity attacks and compromises are found and analyzed,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE>. [↑](#footnote-ref-8)
8. NIST CSF 2.0 via CPRT, “PR.PS-02: Software is maintained, replaced, and removed commensurate with risk,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-02>. [↑](#footnote-ref-9)
9. NIST CSF 2.0 via CPRT, “GV.RR-04: Cybersecurity is included in human resources practices,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.RR>. [↑](#footnote-ref-10)
10. 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-11)
11. 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-12)
12. 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-13)
13. NIST CSF 2.0 via CPRT, “DE.CM-03: Personnel activity and technology usage are monitored to find potentially adverse events,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM-03>. [↑](#footnote-ref-14)
14. 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-15)
15. CISA, “Stop Ransomware,” <https://www.cisa.gov/stopransomware>. [↑](#footnote-ref-16)
16. Eric Bedner, “International extortion group claims to have confidential information in month-long cyber attack on CT hospitals,” CT Insider, August 30, 2023, <https://www.ctinsider.com/journalinquirer/article/connecticut-hospitals-cyber-attack-18334048.php#:~:text=%22We%20activated%20our%20incident%20response%20protocols%20which%20included,working%20with%20law%20enforcement%20authorities%2C%27%27%20Prospect%20officials%20said.> [↑](#footnote-ref-17)
17. Pat Eaton-Robb, “A cyberattack has disrupted hospitals and health care in five states,” ABC News, August 4, 2023, <https://abcnews.go.com/Health/wireStory/cyberattack-disrupted-hospitals-health-care-states-102017847>. [↑](#footnote-ref-18)
18. Steve Alder, “Managed Care of North America Hacking Incident Impacts 8.9 Million Individuals,” The HIPPA Journal, August 29, 2023, <https://www.hipaajournal.com/managed-care-of-north-america-hacking-incident-impacts-8-9-million-individuals/>. [↑](#footnote-ref-19)
19. Steve Alder, “Medical Records from Prospect Ransomware Attack Appear on Dark Web,” The HIPPA Journal, May 30, 2023, <https://www.hipaajournal.com/medical-records-from-prospect-ransomware-attack-appear-on-dark-web/>. [↑](#footnote-ref-20)
20. “Major Dental Insurer MCNA Dental Suffers Devastating Ransomware Attack,” The Healthcare Technology Report, June 13, 2023, <https://thehealthcaretechnologyreport.com/major-dental-insurer-mcna-dental-suffers-devastating-ransomware-attack/>. [↑](#footnote-ref-21)
21. Alder, “Managed Care of North America Hacking Incident.” [↑](#footnote-ref-22)
22. “Crowe v. Managed Care of North America, Inc. Docket No. 0:23-cv-61065,” Court Docket, June 05, 2023, <https://www.bloomberglaw.com/public/desktop/document/CrowevManagedCareofNorthAmericaIncdbaMCNADentalDocketNo023cv61065/1?doc_id=X1Q6OJJ1BO82>. [↑](#footnote-ref-23)