

**[Enter Organization Name]**

**CISA Tabletop Exercise Package**

**K-12 Schools**

## <Insert Date>

## Cybersecurity and Infrastructure Security Agency

Updated September 2023

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 13](#_Toc143606192)

[Appendix B: Acronyms 16](#_Toc143606193)

[Appendix C: Case Studies 17](#_Toc143606194)

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

[Appendix E: Contacts and Resources 20](#_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 the cyber resilience of <name of school or district> and their ability to respond to a significant cyber incident. | |
| National Institute of Standards and Technology Cybersecurity Framework | Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess cybersecurity policies, procedures, and processes to manage cybersecurity risk. 2. Evaluate the efficacy of organizational cybersecurity education and training. 3. Discuss organizational resilience through risk management, back-up procedures, and recovery/restoration capabilities. | |
| Threat or Hazard | Phishing, Ransomware | |
| Scenario | A threat actor targets <your school/district> employees through phishing emails as an entry point into networks/systems. Attackers compromise Personally Identifiable Information (PII) and install ransomware on <your school/district> computers. | |
| 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 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 administrators and principals.

**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 CISA cyber threat alert for K-12 institutions, the contentious firing of a staff member, and a suspicious email.
  + **Module 2:** This module includes a ransomware attack affecting school networks, media inquiries, and data exfiltration affecting student records.
* 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) and the Federal Bureau of Investigation (FBI) issue a joint alert[[2]](#footnote-3) regarding a rise in cyberattacks targeting K-12 educational institutions. The alert describes the tactics, techniques, and procedures (TTPs)[[3]](#footnote-4) used by cyber criminals, including phishing emails, ransomware, remote hacking, distributed denial of service (DDoS) attacks, and data exfiltration from schools. Cyber threat actors view schools as targets of opportunity and these attacks are expected to continue through the academic year.

### Day 7

An administrative staff member is fired for frequent, unexplained absences. The staff member creates a public and unprofessional commotion while leaving the building.[[4]](#footnote-5)

### Day 9

An urgent email, which appears to be from Human Resources, instructs employees to update their banking information in the district payroll system. The email states that employees who fail to update their information may not receive their next paycheck on time. When users click the email link, it takes them to a page that resembles the <your district*>* website and prompts them to log in using their employee credentials.[[5]](#footnote-6)

### Day 10

Laptops are issued to students and teachers at <your school’s name>. Teachers pick up their designated laptop and begin setting up their classrooms. A few teachers use the default passwords rather than creating their own.[[6]](#footnote-7)

### Day 30

Following the most recent pay date, a report from Human Resources indicates that 38 employees did not receive their paychecks, despite having up-to-date account information and direct deposit enabled for their accounts. IT staff receive an unusually high number of reports from faculty and staff who are unable to access their employee accounts. Staff members are seeing error messages stating their credentials are invalid or their accounts no longer exist in the system.[[7]](#footnote-8)

## 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. How would you describe <your school/district’s> cybersecurity posture?
   1. How frequently are users required to change their passwords?
   2. Does <your school district/county> utilize multi-factor authentication (e.g., something you know, something you have, something you are) to mitigate the potential effects of phishing?
3. Describe your organization’s cybersecurity training program for employees and school board members.
   1. How often are employees and school board members 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?
4. How do users report suspicious emails?
   1. What is the process for employees, students, and parents/guardians to report suspicious emails?
   2. What procedures or plans would be followed once a suspicious email has been reported?
5. What cybersecurity threat information does your organization receive?
   1. What cyber threat information is most useful?
   2. How is information disseminated throughout your organization and by whom?
   3. 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 school functions?
   2. Describe your organization’s asset management plan and explain how you prioritize critical assets.
   3. What improvements have been implemented to enhance cyber resilience after conducting recent risk assessments?
   4. Do you have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
7. Discuss your risk management strategy.
8. How is it developed/maintained?
9. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[8]](#footnote-9)
10. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
11. Does your organization have backups of vital records?
12. How are they stored (quantity, location, etc.)?
13. How frequently do you run backups?
14. How long do you keep copies of archived files backed up?
15. How long would it take to restore primary files from backups?
16. What are your onboarding and offboarding processes for granting employees network access?

# Module 2

### Day 46

Faculty and staff who are still logged in to the system cannot access their school emails, curriculum materials, or student grades on their local drives or the online school platform/learning management system. They are presented with the following message on their devices:

“We own your data. For $350,000 in cryptocurrency, your files will be returned. Submit payment to the wallet below within 96 hours, or everything will be posted for sale to the highest bidder. Don’t believe us? We will publish some of your data every 24 hours.”

### Day 47

The attackers publish a sample of exfiltrated student data from your school on the dark web. They also claim they will release more data every 4 hours until the ransom is paid.

A screenshot of the data includes student names, telephone numbers, and addresses.[[9]](#footnote-10)

### Day 48

Families affected by the data breach angrily call their child’s school, board member offices, and the Superintendent’s office looking for answers.

### Day 49

Your local news outlet calls <your school/district/county> asking for comments on the ransomware incident and impacts on student learning. Several parents/guardians have been interviewed by the news outlet and express concerns for their students’ safety.

## Discussion Questions

1. Based on your cyber incident response plan (CIRP) or incident response plan, what actions would your <school/district/county> take to minimize the incident’s impact on current school operations?
   1. How long can you maintain alternative procedures for student instruction and essential functions?
   2. When would you consider instructing staff and students not to use school-issued devices?
   3. How long would it take to recover and restore impacted systems?
   4. When would a cyber incident prompt you to plan for changes to the academic calendar?
2. Explain your organization’s decision-making process regarding ransomware payment.[[10]](#footnote-11)
   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 the advantages and disadvantages of either agreeing or refusing to pay.
   4. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
3. Would the release of sensitive information or PII require specific actions during incident response and recovery?
4. How would <your school/district/county’s> Communications/Public Information personnel respond to the complaints and concerns from parents/guardians?
   1. How would <your school/district/county> address these incidents with the local media?
5. How sufficient are <your school/district/county’s> current internal resources for responding to the cyber incidents in this scenario?
   1. What additional resources outside of your organization are necessary for responding to the cyber incident?
   2. What are the processes or procedures for requesting additional resources?
   3. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
6. 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. 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 page, 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 <school/district/county>’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 cybersecurity language is included within third-party vendor contracts?
9. How do you evaluate the cybersecurity posture of your vendors?
10. How often are contracts reviewed?
11. How do your service level agreements address cyber incident notification?
12. What level of access do your third-party vendors have to your <school/district/county> network?
13. What mechanisms or processes are in place to prevent malicious activity?
14. Describe your patch management plan.
15. What risk assessments are performed on network servers?
16. What processes are in place to proactively evaluate each server’s criticality and applicability to software patches?
17. What considerations are addressed in the plan’s risk management strategy (e.g., extended downtime, loss of data, impaired functionality, etc.)?
18. What is your method for tracking and identifying firmware vulnerabilities in your network?
19. How are IT and business continuity functions coordinated with physical security?
20. 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?
21. How is the integrity of your critical data protected and validated?
22. What external entities have access to the database?
23. How do those entities report a breach of their systems to your office?
24. What mission essential functions are impacted by the incidents described in the scenario?
25. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
26. If primary communications are compromised, how do you provide information to internal and external entities?
27. What policies and procedures does <your school/district/county> use to decide when and how to restore backed-up data?
    1. How does your <your school/district/county> incorporate measures for ensuring the integrity of backup data before restoration?

## Employee and Student Accounts & Privileges

1. Describe your <your school/district/county>’s bring your own device (BYOD) policy.
2. What are your organization’s policies or procedures for IT account management?
3. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

## Incident Identification

1. How are cyber incidents reported within <your school/district/county>?
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 school/district/county>’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. Describe your <your school/district/county>’s ability to monitor the Dark Web.
11. How often is your organization’s data reviewed?
12. 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 breach of <vendor> affect <your school/district/county> if they have access to your information?
5. What are the notification requirements to <your school/district/county> for breaches?
6. At what point would you notify your local, State Board of Education and/or U.S. Department of Education?

## Recovery

1. When does <your school/district/county> 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 school/district/county> 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?
2. How often does your organization exercise its CIRP?
3. How do <your school/district/county>’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 school/district/county> what cybersecurity resilience goals have you set?
2. What cybersecurity training is required for senior administrative staff/school board members?
3. What is your role during a cyber incident?
4. What information do you need to support your decision-making process?
5. What are the gaps in your cybersecurity workforce?
   1. How does your <your school/district/county> recruit, develop, and retain cybersecurity staff?
6. What state, local, tribal, territorial, or regional partners do you enlist for cybersecurity personnel support?

## Public Information

* + - 1. What training is provided to employees regarding reporting any contact with the media to the appropriate public information personnel?
      2. How do you build and maintain trust with your students and parents/guardians?

## 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 |
| BYOD | Bring Your Own Device |
| DDoS | Distributed Denial of Service |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| PHI | Protected Health Information |
| PII | Personally Identifiable Information |
| TLP | Traffic Light Protocol |
| ZTA | Zero Trust Architecture |

# Appendix C: Case Studies

## Medusa Ransomware Attack

In March 2023, a large school system suffered a ransomware attack. Stolen files were posted online by the hacker group Medusa following an announcement by the school system to the public and the refusal to pay the one-million-dollar ransom. The file cache totaled over 200,000 files and contained highly sensitive information, such as allegations of teacher abuse, student psychological reports, district finances, and special education reports. Medusa also posted stolen information on Twitter and Facebook, including a 50-minute video of file screenshots.[[11]](#footnote-12)

The Medusa ransomware group encrypted the files with a MEDUSA file extension.[[12]](#footnote-13) The group’s operations began in 2021; however, this 2023 attack was their first major attack as an organization. The group utilizes the “Medusa Blog” to release the data of victims who choose not to pay the ransom.

## Royal Ransomware Attack

A large school district suffered a Royal ransomware attack in January 2023. Teachers lost all network and internet access. On the morning of the attack, teachers discovered a ransom letter printed from district printers in various schools across the district.[[13]](#footnote-14) Initially, school officials did not suspect that any sensitive data was lost. However, in March 2023, the district sent a letter to employees notifying them that confidential data, including social security numbers, had been stolen.[[14]](#footnote-15)

According to a joint statement from CISA and the FBI, Royal ransomware employs its own custom-made file encryption program. Upon gaining access, Royal actors disable antivirus software and exfiltrate large amounts of data before ultimately deploying the ransomware and encrypting the systems. Royal actors do not include ransom amounts and payment instructions as part of the initial ransom note. Instead, the note, which appears after encryption, requires victims to directly interact with the threat actor.[[15]](#footnote-16)

## Business Email Compromise

A school system fell victim to a business email compromise that led to the authorization of bank transfers totaling $6 million to hackers in June 2023. Malicious actors gained access to the Chief Operating Officer’s email address and surveilled their email traffic for weeks, subsequently sending email requests for electronic money transfers to real vendors contracted by the school system, however the account routing information was fraudulent. The school system discovered the requests were fraudulent when one vendor, a school bus company, informed the school system that they missed expected payments. Upon discovery of the thefts, the school system suspended all electronic payments except for employee payroll.[[16]](#footnote-17)

The school system did not publicly disclose the thefts until two months after they occurred while the FBI investigated the case. As of August 2023, the FBI recovered $3.6 million, and the case is ongoing. The school system stated they are working with third party experts to fortify their systems.[[17]](#footnote-18)

## Social Engineering – Phishing

In July 2021, a university healthcare organization disclosed that it had experienced a data breach caused by a phishing attack. Threat actors were able to obtain valid credentials though malicious emails sent to employees.[[18]](#footnote-19) Using the gathered stolen credentials, the threat actors gained unauthorized access to the organization’s emails from December 2020 to April 2021. The organization reported that the PII and protected health information (PHI) of nearly 500,000 employees, patients, and students may have been compromised.[[19]](#footnote-20) This information included names, social security numbers, and medical images and diagnoses. The incident was reported to the Federal Bureau of Investigation (FBI), and the organization has since enhanced its security controls.

# 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.

## 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 (<https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing>)

# Appendix E: Contacts and Resources

Federal Government Resources

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* Department of Education Student Privacy Policy Office (contact: <https://studentprivacy.ed.gov>, [PrivacyTA@ed.gov](mailto:PrivacyTA@ed.gov), 855-249-3072)
* 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/>)

K-12 Preparedness Resources

* CISA Partnering to Safeguard K-12 Organizations from Cybersecurity Threats (<https://www.cisa.gov/resources-tools/resources/report-partnering-safeguard-k-12-organizations-cybersecurity-threats>)
* CISA State and Local Cybersecurity Grant Program (<https://www.cisa.gov/state-and-local-cybersecurity-grant-program>)
* CISA Cross-sector Cybersecurity Performance Goals (<https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist>)
* NIST Cybersecurity Framework Tools (<https://csf.tools/>)
* SchoolSafety.gov Cybersecurity (<https://www.schoolsafety.gov/cybersecurity>)
* Department of Education/CISA K-12 Digital Infrastructure Brief: Defensible and Resilient (<https://tech.ed.gov/infrastructure/>)
* Department of Education Readiness and Emergency Management for Schools Cybersecurity Considerations for K-12 Schools and School Districts (<https://rems.ed.gov/trainings/CourseCybersecurity.aspx>)
* Educause Cybersecurity Program (<https://www.educause.edu/focus-areas-and-initiatives/policy-and-security/cybersecurity-program>)
* The K12 Security Information exchange (K12 SIX) Incident Response Runbook (<https://www.k12six.org/s/K12SIX-IncidentResponseRunbook.pdf>)
* Ransomware:
  + 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>)
  + Ransomware: Targeting Educational Institutions (<https://fsapartners.ed.gov/sites/default/files/2022-06/H-052_Ransomware_Targeting_Educational_Institutions_AB_061622_FINAL.pdf>)

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 CSF Tools, “Security Alerts, Advisories, and Directives,” <https://csf.tools/reference/nist-sp-800-53/r5/si/si-5/> [↑](#footnote-ref-3)
3. CISA CPG Checklist, “3.A Detecting Relevant Threats and TTPs,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-4)
4. CISA CPG Checklist, “2.D Revoking Credentials for Departing Employees,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-5)
5. CISA CPG Checklist, “2.I Basic Cybersecurity Training,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-6)
6. CISA CPG Checklist, “2.A Changing Default Passwords,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-7)
7. CISA CPG Checklist, “2.S Incident Response (IR) Plans,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-8)
8. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model> [↑](#footnote-ref-9)
9. NIST CSF Tools, “Data Security,” <https://csf.tools/reference/nist-cybersecurity-framework/v1-1/pr/pr-ds/> [↑](#footnote-ref-10)
10. CISA, “Stop Ransomware,” <https://www.cisa.gov/stopransomware> [↑](#footnote-ref-11)
11. Kevin Collier, “Students’ psychological reports, abuse allegations leaked by ransomware hackers,” *NBC News****,*** April 26, 2023, <https://www.nbcnews.com/tech/security/students-psychological-reports-abuse-allegations-leaked-ransomware-hac-rcna79414>. [↑](#footnote-ref-12)
12. # Sead Fadilpašić, “The Medusa Ransomware Group is Getting Serious,” *TechRadar,* March 13, 2023,

    <https://www.techradar.com/news/the-medusa-ransomware-group-is-getting-serious>. [↑](#footnote-ref-13)
13. Mikala Novitsky, “Southern Arizona’s Largest School District Hit by Cyber Attack,” *13 News,* January 30, 2023, <https://www.kold.com/2023/01/31/southern-arizonas-largest-school-district-hit-by-cyber-attack/>. [↑](#footnote-ref-14)
14. Bivian Contreras, “TUSD Provides Update on Ransomware Attack Investigation,” *KGUN9 ABC*, April 18, 2023, <https://www.kgun9.com/news/local-news/tusd-provides-update-on-ransomware-attack-investigation>. [↑](#footnote-ref-15)
15. Cybersecurity and Infrastructure Security Agency, “#StopRansomware: Royal Ransomware,” <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-061a>. [↑](#footnote-ref-16)
16. Lola Fadulu, “Hackers Stole $6 Million from the New Haven School System,” *The New York Times*, August 10, 2023, <https://www.nytimes.com/2023/08/10/nyregion/new-haven-schools-hackers.html>. [↑](#footnote-ref-17)
17. “Connecticut School District lost more than $6 million in cyber attack,” *Associated Press,* August 10, 2023, <https://apnews.com/article/connecticutt-school-district-cyber-attack-new-haven-f7fad8a63916a1a80a3885a92d326964>. [↑](#footnote-ref-18)
18. S. Gatlan, “UC San Diego Health discloses data breach after phishing attack,” BleepingComputer, July 27, 2021, <https://www.bleepingcomputer.com/news/security/uc-san-diego-health-discloses-data-breach-after-phishing-attack/>. [↑](#footnote-ref-19)
19. Mike Freeman, “UC San Diego Health sued over data breach that may have exposed records of 500,000 patients,” *San Diego Union-Tribune*, September 24, 2021, <https://www.sandiegouniontribune.com/business/story/2021-09-23/sd-fi-ucsandiego-cyber-attack#:%7E:text=UC%20San%20Diego%20Health%20faces%20a%20lawsuit%20over,and%20others%20connected%20with%20the%20health%20care%20system>. [↑](#footnote-ref-20)