

**CISA Tabletop Exercise Package Elections – Voting Machine Compromise**

[Enter Organization Name]

<Exercise Date>

Updated January 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc148091387)

[Exercise Overview 5](#_Toc148091394)

[General Information 6](#_Toc148091395)

[Module 1 8](#_Toc148091396)

[Module 2 11](#_Toc148091397)

[Appendix A: Additional Discussion Questions 14](#_Toc148091398)

[Appendix B: Acronyms 17](#_Toc148091399)

[Appendix C: Case Studies 18](#_Toc148091400)

[Appendix D: Malicious Activity 19](#_Toc148091401)

[Appendix E: Contacts and Resources 21](#_Toc148091402)

# Handling Instructions

Delete instructions that are not applicable.

TLP:CLEAR

The title of this document is <Exercise Title> Situation Manual (SitMan). 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 (SitMan). 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 (SitMan). This document is unclassified <if applicable> and designated as “*Traffic Light Protocol (TLP):AMBER”:* This designation has 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. **The source is at liberty to specify additional sharing restrictions. These must be adhered to by recipients.**

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 (SitMan). This document is unclassified <if applicable> and designated as *“Traffic Light Protocol (TLP):AMBER+STRICT*. This designation has 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. **The source is at liberty to specify additional sharing restrictions. These must be adhered to by recipients.**

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 (SitMan). 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 Schedule | 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 identification, protection, and response capabilities for cyber security incidents impacting <state/county/municipality>’s elections infrastructure. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Assess election officials' ability to identify, respond to, and recover from cybersecurity incidents. 2. Inform the development or refinement of policies, plans, and procedures to increase the resilience of <state/county/municipality> elections infrastructure. 3. Explore processes for sharing accurate elections information. | |
| Threat or Hazard | Voting Machine Tampering, Ransomware | |
| Scenario | * Disruption and compromise of election equipment * Ransomware impacting election offices * Impacts on voter confidence | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of participating organizations in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact info | **National Cyber Exercise Program**  [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 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. Suggested players include representatives from the IT, elections, communications, and legal departments, and any personnel with real-world cyber incident response roles. Players should bring a copy of their Cyber Incident Response Plan (CIRP) and any other incident related plans, policies, and procedures to the exercise.

**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 representatives from the IT, elections, communications, human resources (HR), and legal departments as well as leadership who do not have assigned real-world cyber incident response roles but may be involved in response efforts or have a need-to-know.

**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 facilitated exercise. Players will participate in the following:

* Cyber threat briefing (if desired)
* Scenario modules:
  + **Module** **1:** This module introduces alerts and events regarding a phishing campaign targeting voting machine companies. There is also a vendor email regarding software and firmware updates and rumors about unsecure voting equipment.
  + **Module 2:** The final module includes broken seals on voting equipment, issues related to ballot marking and voting processes, incorrect vote counts followed by news media and voter inquiries.
* 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 local government’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

### 50 Days Prior to Election

The Elections Infrastructure Information Sharing & Analysis Center (EI-ISAC) forwards a joint alert released by CISA and the Federal Bureau of Investigation (FBI) warning of increased threats targeting U.S. elections infrastructure leading up to the general election.[[2]](#footnote-3) The alert describes a phishing campaign targeting voting system vendors and other third-party services. Once the malicious actors gain access to vendors/service providers, emails are sent to customers using false system updates in order to lure users into downloading a malware package onto their system.

### 35 Days Prior to Election

Election employees receive an email from <voting system vendor [e.g., Election Management System (EMS)]>. The email includes an attachment with new guidance on performing updates to voting system software and firmware updates for <tabulators, Ballot Marking Devices (BMDs), Direct Recording Electronic (DRE) voting systems>. Some employees report the email as suspicious to the Information Technology (IT) Department/Help Desk while others download the attachment to review the vendor’s guidance, and find a blank document.[[3]](#footnote-4)

### 19 Days Prior to Election

As early voting begins, IT staff discover several remote login attempts on <state/county/municipality> systems using specific combinations of usernames and passwords. Additionally, the network intrusion detection system alerted that various state and local agencies, including elections offices, had an unusual number of port scans by unknown entities.[[4]](#footnote-5)

### 15 Days Prior to Election

Security researchers discover copies of software code for <insert specific EMS relevant to your county/municipality (e.g., voter registration, results reporting, etc.)> from one of your vendors posted on the dark web. The site is selling software exploitations to those who wish to “have some fun this election season.”[[5]](#footnote-6)

The researchers report this information to the vendor, who then alerts CISA and EI-ISAC. Later, the vendor updates its customer base and relevant stakeholders, urging them to immediately install a patch to address the vulnerability. Local news media begins to cover the story and seeks comments from <elections officials/staff, Secretary of State office, etc.> on the potential impacts this could have on the upcoming election.[[6]](#footnote-7)

## 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 the elections process?
2. Discuss <state/county/municipality>’s cyber resilience planning.[[7]](#footnote-8)
   1. What risk assessments have you conducted to identify specific cyber threats, vulnerabilities, and critical assets?[[8]](#footnote-9)
   2. Describe your asset management plan and how you prioritize critical assets.
   3. What improvements have you implemented to enhance cyber resilience following recent risk assessments?
   4. Do you apply Zero Trust Architecture (ZTA)/zero-trust concepts?[[9]](#footnote-10)
3. What cybersecurity threat information does <state/county/municipality> receive?
   1. What cyber threat information is most useful?
   2. How is information disseminated across your organization and by whom?
   3. What actions would your organization take following an alert like the one presented in the scenario?
4. Describe <state/county/municipality> cybersecurity training program for employees.[[10]](#footnote-11)
   1. How often are employees required to complete this training?
   2. Is training required during employee onboarding before granting system/network access?
   3. What additional training is required for employees who have system administrator-level privileges?
   4. What type of training methods or approaches have you found most beneficial?
5. 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?
6. Describe your <state/county/municipality> inventory process for election hardware and software.[[11]](#footnote-12)
   1. Describe the process for updating both the hardware and software.
   2. What security requirements do you have as part of your contracts/service-level agreements with your third-party vendors?
7. How does <state/county/municipality> baseline network activity?[[12]](#footnote-13)
   1. How do you distinguish between normal and abnormal traffic?
8. Does your <state/county/municipality> have backups of vital records stored in a location separate from your primary working files/copies?[[13]](#footnote-14)
9. How frequently do you run backups?
10. How long do you keep copies of archived files backed up?
11. How long would it take to restore primary files from backups?
12. How often do you practice restoring from backups?

# Module 2

### 13 Days Prior to Election

When <state/county/municipality> <employees/election staff> arrive at work and attempt to login to their computers, the following message is displayed:

**“Thanks for locking yourself out! Pay $XXX,000 in Bitcoin or your system will be wiped clean!! Time is ticking away and you have 48 hours to pay!!”**

The computers are locked and their contents are encrypted by ransomware.[[14]](#footnote-15)

### Election Day – Morning

Poll workers at several voting locations across the <state/county/municipality> find seals covering media ports of voting equipment broken. There are no other signs of tampering, but early assessments indicate that the seals are broken on at least <20 percent> of the equipment in your largest precincts.[[15]](#footnote-16)

<A poll worker> posts images of the broken seals on social media and claims that they saw a USB drive near one of the machines. These posts quickly circulate on various social media platforms with voters replying that this is proof the results will not be accurate.

### Election Day – Afternoon

Several voters in one of the largest counties/municipalities in your state claim that <[they are not able to select or mark their desired candidate] or [their candidate is not present on the printed ballot]>. At other locations, there are allegations that the voter’s verified printed ballot does not match their selection made on the screen of the ballot marking device. These instances lead to significant delays at multiple voting locations.[[16]](#footnote-17)

As the afternoon progresses, local news outlets report on the various issues occurring at voting locations across the <state/county/municipality>.

Election Day – Evening

As <state/county/municipality> begins reporting unofficial election night results, local media outlets report alleged incidents of incorrect vote counts. County and state elections offices receive several calls from local media and voters seeking comment.[[17]](#footnote-18)

## Discussion Questions

1. Using your Cyber Incident Response Plan (CIRP), describe the actions your organization would take to respond to the ransomware attack.[[18]](#footnote-19)
   1. How often is the CIRP exercised with incident response personnel?
   2. What guidance does the plan include on assessing the severity of the incident?
   3. How does incident severity level dictate response?
   4. How are critical systems and processes incorporated into your CIRP?
2. What capabilities and resources are required for responding to this scenario?[[19]](#footnote-20)
3. What additional resources outside of your organization would be necessary for responding to the cyber incident?
4. What are the processes or procedures for requesting additional resources?
5. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
6. Explain your organization’s decision-making process regarding ransomware payment.[[20]](#footnote-21)
   1. Are ransomware policies/procedures included in your CIRP?
   2. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
   3. Describe the impact the sale or release of sensitive information or PII would have on your response and recovery activities.
7. What security breach notification laws are you subject to?[[21]](#footnote-22)
8. How would you address delays at polling locations?
9. Describe employee and poll worker social media policies.
10. What processes or procedures do you have to secure and verify election equipment seals before and after an election?
    1. How would you respond to the broken equipment seals?
    2. How would you respond to the USB drive in a voting machine?
11. How does your <state/county/municipality> conduct logic and accuracy testing of electronic ballot marking devices and tablution systems before the voting period?
12. Describe your organizational processes to respond to the media reports and inquiries.[[22]](#footnote-23)
    1. How do you ensure the public has accurate elections information?
    2. Do you have holding statements that are available to leverage for communicating with the media and public?
    3. How would you preserve and reinforce the public’s confidence and trust in your <state/county/municipality> during a significant incident?
13. What changes will you implement to increase the resilience of your organization?[[23]](#footnote-24)

# 

# 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 do you integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
3. Discuss your supply chain concerns related to cybersecurity infrastructure.
4. What cybersecurity language is included within third-party vendor contracts?
5. How do you evaluate the cybersecurity posture of your vendors?
6. How often are contracts reviewed?
7. How do your service level agreements address cyber incident notification?
8. What level of access do your third-party vendors have to your network?
9. Describe your patch management plan.
10. What considerations (e.g., extended downtime, loss of data, impaired functionality, etc.) are addressed in the plan’s risk management strategy?
11. What is your method for tracking and identifying vulnerabilities in your network?
12. How are IT and business continuity functions coordinated with physical security?
13. What processes do you have to ensure that your external dependencies (e.g., contractors, power, water, etc.) are integrated into your security and continuity plans?
14. How is the integrity of your critical data protected and validated?
15. How would those entities report a breach of their systems to your office?
16. How does <state/county/municipality> maintain availability of key assets (e.g., network connectivity, etc.)?
17. If primary communications are compromised, how do you provide information to internal and external entities?
    1. What is your organization’s communications primary, alternate, contingency and emergency (PACE) communications plan?
18. What policies and procedures do you use to decide when and how to restore backed-up data?
    1. How do you incorporate measures for ensuring the integrity of backup data before restoration?

## Accounts & Privileges

1. Describe your bring your own device (BYOD) policy.
2. What are your 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 <state/county/municipality>?
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. When are other <state/county> offices notified?
9. Discuss your intrusion detection capabilities and analytics that alert you to a potential cyber incident.
10. What type of hardware and/or software do you use to detect and prevent malicious activity on your systems/network?
11. How often is your data reviewed? How would you determine whether unauthorized manipulation of data has occurred?

## Incident Response

1. What are the roles of your network operations center/security operations center during a cyber incident?
2. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
3. At what point would you contact the state’s chief election official (Secretary of State and/or State Election Director)?
4. At what point in the scenario would you contact law enforcement?

## Recovery

1. What actions would you take if IT/incident response staff could not confirm the integrity of your systems/data?
2. What is the risk associated with re-activating critical business processes and systems?
3. How long and costly would the process be to completely rebuild these systems?
4. 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 do your training and exercise efforts address both physical and cyber risks?
   1. Have senior staff participated in a cybersecurity exercise?

## Senior Leaders

1. As a leader in <state/county/municipality>, what cybersecurity resilience goals have you set?
2. What cybersecurity training is required for senior leadership?
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?
6. How does <state/county/municipality> recruit, develop, and retain cybersecurity staff?

## 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 the public?

## Legal

1. What is the role of the legal department during a cyber incident?
2. What legal issues need to be addressed based on the scenario?
3. What legal documentation should <state/county/municipality> have for cyber incidents?

# Appendix B: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BMD | Ballot Marking Device |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cross-Sector Cybersecurity Performance Goals |
| DRE | Direct Recording Electronic (voting machine) |
| EI-ISAC | Elections Infrastructure Information Sharing and Analysis Center |
| EMS | Election Management System |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| IS | Information Systems |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| TLP | Traffic Light Protocol |

# Appendix C: Case Studies

## Ballot Tabulation Machine Malfunction

During the midterm elections in November 2022, 60 county voting centers were affected by a ballot tabulation machine technical error.[[24]](#footnote-25) Printers would not mark the ballots dark enough for vote-counting machines to read them. The county switched to manual processes, having voters cast their ballots by dropping them in secure slots to be manually counted. The technical error sparked social media claims of widespread voter fraud. The Election Integrity Partnership observed more than 40,000 social media posts regarding the error in a span of two hours. Election officials assured the public that the technical error did not affect the accuracy of the results and did not prevent anyone from voting.[[25]](#footnote-26)

## Voting Tabulation System Installation Error

In November 2022, a voting tabulation system error caused the double counting of votes in six voting districts in a county. The error led to a change in the initial tablulated results of a local school board race. A third-party vendor responsible for voting machine maintenance reinstalled the voting tabulation software in July of 2022. However, they failed to ensure that the Universal Serial Bus (USB) flash drives containing votes could only be uploaded once.[[26]](#footnote-27) The problem was not detected during the post-election audit of the system.

## Ransomware Attacks on Elections Infrastructure

In October 2020, a county suffered a ransomware attack against their systems. The incident impacted the accessibility of the county’s voter signature database, as well as the voting precinct map hosted on the county website. While attackers did not specifically target elections operations, the loss of access to the voter signature database significantly delayed absentee ballot processing. County officials were able to verify voter signatures using paper copies of voter registration cards and voting processes remained unaffected by the ransomware attack. Even though the state election network was unaffected, the attack raised concerns regarding the potential impacts of ransomware on election-related infrastructure systems.[[27]](#footnote-28),[[28]](#footnote-29)

# Appendix D: Malicious Activity

## Ransomware

Ransomware is a type of malicious software designed to deny 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. Ransomware typically spreads through phishing emails or by users 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. For elections, ransomware could leak or deny access to voter registration data, unofficial results reporting, and other sensitive information. It could also impact access to important election systems during critical operational periods, such as registration and candidate filing deadlines. 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

* Cybersecurity Toolkit and Resources to Protect Elections (<https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>)
* 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 cyber threat actors use to exploit network and system vulnerabilities is social engineering, the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. A common social engineering technique involves the use of phishing. Phishing uses email, text messaging, and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Social engineering is effective for compromising networks and evading intrusion detection systems without leaving a log trail. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, providing instruction on where to forward them, and keeping software and systems up to date. Organizations can also implement software designed to safeguard sensitive information, detect unsafe URLs, block phishing websites, detect known phishing and malware, and implement Multi-Factor Authentication (MFA) to guard against the use of stolen credentials.

### Additional Resources

* Cybersecurity Toolkit and Resources to Protect Elections (<https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>)
* 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>)

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 Complaint 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)

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))
* CISA Cybersecurity Toolkit and Resources to Protect Elections (<https://www.cisa.gov/cybersecurity-toolkit-and-resources-protect-elections>)
* CISA Guide to Operational Security for Election Officials (<https://www.cisa.gov/resources-tools/resources/guide-operational-security-election-officials>)
* SLTT:
  + State and Local Cybersecurity Grant Program (<https://www.cisa.gov/state-and-local-cybersecurity-grant-program>)
  + CISA CDM Program (<https://www.cisa.gov/resources-tools/programs/continuous-diagnostics-and-mitigation-cdm-program>)
  + CISA Find Help Locally (<https://www.cisa.gov/audiences/find-help-locally>)
* Elections Infrastructure Information Sharing and Analysis Center (<https://www.cisecurity.org/ei-isac>)

Resources for State and Local Government Entities

* Multi-State Information Sharing and Analysis Center (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* National Governors Association (NGA) Resource Center for State Cybersecurity (<https://www.nga.org/statecyber/>)
* 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/>)

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. CISA Cybersecurity Alerts & Advisories, <https://www.cisa.gov/news-events/cybersecurity-advisories>. [↑](#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, “ID.RA-01: Vulnerabilities in assets are identified, validated, and recorded,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-01>. [↑](#footnote-ref-5)
5. NIST CSF 2.0 via CPRT, “RS.CO-03: Information is shared with designated internal and external stakeholders,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO-03>. [↑](#footnote-ref-6)
6. 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-7)
7. 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-8)
8. NIST CSF 2.0 via CPRT, “ID.AM-05: Assets are prioritized based on classification, criticality, resources, and impact on the mission,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.AM-05> [↑](#footnote-ref-9)
9. CISA Resources, “Zero Trust Maturity Model,” <https://www.cisa.gov/zero-trust-maturity-model>. [↑](#footnote-ref-10)
10. 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-11)
11. NIST CSF 2.0 via CPRT, “ID.AM: Asset Management,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.AM>. [↑](#footnote-ref-12)
12. NIST CSF 2.0 via CPRT, “PR.PS-01: Configuration management practices are established and applied,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-01>. [↑](#footnote-ref-13)
13. 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-14)
14. NIST CSF 2.0 via CPRT, “DE.CM-09: Computing hardware and software, runtime environments, and their data 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-09>. [↑](#footnote-ref-15)
15. NIST CSF 2.0 via CPRT, “RS.MA: Incident Management,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.MA>. [↑](#footnote-ref-16)
16. NIST CSF 2.0 via CPRT, “RC.RP: Incident Recovery Plan Execution,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.RP>. [↑](#footnote-ref-17)
17. NIST CSF 2.0 via CPRT, “RS.CO: Incident Response Reporting and Communication,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO>. [↑](#footnote-ref-18)
18. 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-19)
19. 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-20)
20. CISA, “Stop Ransomware,” <https://www.cisa.gov/stopransomware>. [↑](#footnote-ref-21)
21. NIST CSF 2.0 via CPRT, “RC.CO-3: Information is shared with designated internal and external stakeholders,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO-03>. [↑](#footnote-ref-22)
22. NIST CSF 2.0 via CPRT, “RS.CO: Incident Response Reporting and Communication,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RS.CO>. [↑](#footnote-ref-23)
23. NIST CSF 2.0 via CPRT, “ID.IM: Improvement,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM>. [↑](#footnote-ref-24)
24. J. H. Thompson, “Voting Machine Problems in Arizona Fuel Right-Wing Fraud Claims,” *The New York Times*, November 11, 2022, <https://www.nytimes.com/2022/11/08/us/politics/maricopa-voting-problems.html>. [↑](#footnote-ref-25)
25. Eric Ortiz, “Vote machine glitch roils Arizona's Maricopa County and fuels false statements,” *NBC News,* November 8, 2023, <https://www.nbcnews.com/politics/2022-election/vote-machine-glitch-roils-arizonas-maricopa-county-fuels-false-stateme-rcna56261>. [↑](#footnote-ref-26)
26. New Jersey School Board Association, “Monmouth County Election Offices: Error Could Change the Result in Ocean Township’s Board of Education General Election,” last modified January 18, 2023, <https://www.njsba.org/news-publications/school-board-notes/january-18-2023-vol-xl-no-22/monmouth-county-election-offices-error-could-change-the-result-in-ocean-townships-board-of-education-general-election/>. [↑](#footnote-ref-27)
27. Megan Reed, “How Hall County is Handling Influx of Absentee Voting, Effects of Ransomware Attack on Elections Office,” *The Gainesville Times*, October 23, 2020, <https://www.gainesvilletimes.com/news/politics/how-hall-county-handling-influx-absentee-ballots/>. [↑](#footnote-ref-28)
28. Richard Forno, “Ransomware Can Interfere with Elections and Fuel Disinformation – Basic Cybersecurity Precautions Are Key to Minimizing the Damage,” *Government Technology,* accessed February 23, 2021, <https://www.govtech.com/security/Ransomware-Can-Interfere-with-Elections-and-Fuel-Disinformation--Basic-Cybersecurity-Precautions-Are-Key-to-Minimizing-the-Damage.html>. [↑](#footnote-ref-29)