[Enter Organization Name]

CISA Tabletop Exercise Package

Elections – Vote by Mail

Updated October 2022

<Exercise Date>

<Exercise Title>
Situation Manual

Table of Contents

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*": Disclosure is not limited. Sources may use TLP:CLEAR 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 distributed 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, restricted to the community. Sources may use TLP:GREEN when information is useful for the awareness of all participating organizations as well as with peers within the broader community or sector. Recipients may share TLP:GREEN information with peers and partner organizations within their sector or community, but not via publicly accessible channels. Information in this category can be circulated widely within a particular community. **TLP:GREEN information may not be released outside of the 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 share on a need-to-know basis within their organization and its clients. Note that *"TLP:AMBER+STRICT"* restricts sharing to the organization only. Sources may use TLP:AMBER when information requires support to be effectively acted upon, yet carries risks to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may only share TLP:AMBER information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm. Note: if the source wants to restrict sharing to the organization only, they must specify TLP:AMBER+STRICT. **Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to.**

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: 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*": Not for disclosure, restricted to participants only.

Sources may use TLP:RED when information cannot be effectively acted upon by additional parties, and could lead to impacts on a party's privacy, reputation, or operations if misused. Recipients may not share TLP:RED information with any parties outside of the specific exchange, meeting, or conversation in which it was originally disclosed. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting. In most circumstances, **TLP:RED should be exchanged verbally or in person**.

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**
	Time	Activity
	Time	Activity
	Time	Activity
	Time	Activity
Scope	X hour facilitated, discussion-based tabletop exercise	
Purpose	Identify best practices and areas for improvement in incident planning, identification, and response to cyber and physical security threats impacting elections infrastructure.	
INSERT: <NIST, FEMA, or Mission Capabilities>	For example, areas such as Identify, Protect, Respond, etc.	
Objectives	1. Discuss the preparedness of the state and local officials to respond to and manage cybersecurity incidents. 2. Discuss processes for identifying potential cybersecurity incidents or issues. 3. Examine information sharing processes between state and local officials and with external partners. 4. Inform the development of state and local-level processes and plans to address elections-related cyber and physical security incidents.	
Threat or Hazard	Cyber and physical security threat	
Scenario	• Disruption of voter registration information systems • News and social media manipulation related to political candidates and the conduct of elections • Distributed Denial of Service (DDoS) attacks and web defacements impacting board of election websites • Targeting of vote-by-mail process to alter, disrupt, and destroy the voting process • Ransomware and infection of computer systems.	
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 info	National Cyber Exercise Program CISA Exercises CEP@hq.dhs.gov

General Information

Participant Roles and Responsibilities

The term *participant* encompasses many groups of people, not just those playing in the exercise. Groups of participants involved in the exercise, and their respective roles and responsibilities, are as follows:

Players have an active role in discussing or performing their regular roles and responsibilities during the exercise. Players discuss or initiate actions in response to the simulated emergency.
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.
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 will be a multimedia, facilitated exercise. Players will participate in the following:

- Cyber threat briefing (if desired)
- Scenario modules:
    - **Module 1:** This module introduces alerts and events affecting IT users, including an issue with a ballot printing vendor, an unwanted program on users' computers, misinformation, and a phishing email.
    - **Module 2:** This module includes a second issue with a ballot vendor, an abnormally large number of ballot requests, issues with the Secretary of State's (SOS) website, and an inquiry from the media.
    - **Module 3:** The final module includes damaged ballots, website defacements, protesters, news media and social media inquiries, a ransomware demand, and managing concerns around election integrity and loss of voter confidence.
- Hotwash
- ***Structure Note:*** *Injects, 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 will be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario using your knowledge of existing plans and capabilities, and 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 and possible solutions and/or 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.
- The scenario has been developed in collaboration with subject matter experts and exercise planners from your organization.
- In any exercise, assumptions and artificialities are necessary to complete play in the time allotted, to achieve training objectives, and/or account for logistical limitations. Please do not allow these considerations 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

A security company releases an alert on their website describing a cyber campaign against printers and printing companies. The security company believes that attackers are attempting to assemble a new botnet of printers and other Internet of Things (IoT) devices. Once infected, the devices remain available for use in denial of service attacks, or as platforms for further attacker access.

Day 2

The Elections Infrastructure Information Sharing and Analysis Center (EI-ISAC) releases an alert concerning an observed increase in attempts to affect the <mail-in, absentee, vote-by-mail>ballot process. It also highlights disinformation spreading on social media regarding <mail-in, absentee, vote-by-mail> ballots and national public health related issues.

Day 5

A technical alert is released by the Cybersecurity and Infrastructure Security Agency (CISA) and the Federal Bureau of Investigation (FBI) and forwarded by the EI-ISAC regarding a phishing campaign targeting state and local election officials. The alert contains initial indicators of compromise regarding a ransomware payload included in malicious attachments to emails. An observed phishing lure advertises links to the complete series of the hit TV series, <insert TV series name>, on a popular streaming service.

Day 25

Your vendor informs you they are having trouble sourcing the envelope adhesive for your <mail-in, absentee, vote-by-mail> ballot envelopes. The world's main supplier of this envelope adhesive is located abroad in an area where the community is suffering from severe public health issues; it is unclear when they will be able to get a resupply. As a result, your vendor is postponing all orders until they are completely resupplied.

Day 26

A new post by the hacktivist group Hippoponymous claims that they will be targeting the upcoming election in several states. They also claim that they are conducting "completely free penetration testing" for the upcoming election.

Day 27

Employees at your office receive a series of messages from colleagues in other < county, local municipality > departments with links to the < insert TV series name> TV show. These links request that <your entity's> employees install a program to view the upcoming episodes.

Day 28

An employee at your ballot printing vendor receives an email stating that they need to immediately update their payroll and benefit information. The email contains instructions to open the attachment and enable macros to view secure content.

Day 29

Employees in your office notice an unusual program has appeared on their desktops. The program, named ReVue, appears to be a media player that was installed overnight.

When browsing the internet, several employees notice that an excessive number of pop-up ads are appearing on websites. These pop-up ads advertise new links to the <insert TV series name> TV show.

Day 30

The voting period for military and overseas voters begins. One <election official> notices a ballot returned via email requesting that macros be enabled to download secure content. The <election official> accepts the prompt to enable macros and proceeds to process the ballot normally.

Discussion Questions

Discussion questions included in each module may be modified as desired. Additional questions can be found in Appendix A.

1. What actions would your organization take based on the information in Module 1?
    a. What sources of cybersecurity threat intelligence does your organization receive?
2. What plans and processes does your organization to follow in the case of a cybersecurity alert like the one presented in this scenario?
3. If your ballot printing vendor is unable to complete your order for printed ballots, how would you ensure all citizens receive a ballot for <mail-in, absentee, vote by mail>?
4. What other supply chain risks is your office concerned about?
    a. How are you mitigating these risks?
5. How do employees report suspected phishing attempts or other cybersecurity incidents?
    a. What actions does your organization take when suspicious emails are reported?
    b. What are some of the challenges your organization encounters with phishing?
    c. How effective are your organization's methods to protect against phishing?
6. Describe your organization's cybersecurity training programs for employees.
    a. How often are employees required to go through this training?
    b. Are employees allowed to access your networks without completing the required training?
    c. What additional training is required for employees that have access to system-level software?
7. What are your most significant cybersecurity threats and vulnerabilities?
    a. What steps has your organization taken to mitigate risk to your critical systems?
8. What cyber incidents are vendors required to report to your organization?
    a. What is the process and timeline for reporting?
9. How would your organization address the mis/disinformation on social media regarding ballots presented in the EI-ISAC alert?
    a. What can be done to help prevent or mitigate it?
    b. How does your organization communicate with the media?
    c. What additional resources could assist you in combatting misinformation?

Module 2

Day 35

Employees notice that the printed test ballot is different from the electronic ballot file. A candidate's name is missing and the order has been is rearranged.

That same day, an error occurs on the <Chief Election Official's> website. The web page for the <drop box lookup tool> is inaccessible and only shows a blank screen when clicked.

Day 36

Several <counties, municipalities, etc.> have seen an abnormally large number of new voter registrations and registration changes via the online voter registration portal. The volume of requests have increased by <insert percentage>% in comparison to the previous elections. However, the requests appear to contain legitimate citizen information.

Day 37

Your vendor has been able to source new envelope adhesive. They will now be able to produce and deliver envelopes for all of the ballots prior to your deadline.

The <drop box lookup tool> web page on the <Chief Election Official's> website is updated with drop box location information.

Day 47

Voters throughout the state receive envelopes that appear to contain their official ballots. However, some include a candidate representing the Hippoponymous party.

Voters call their <local election office (e.g., County Clerk Office)> and the <State Chief Election Official's> office to question the legitimacy of their ballots.

Later that day, <local election employees (e.g., county clerk)> employees attempting to use the popular search engine, Poogle, are redirected to an unknown merchant's website.

Day 54

A large number of <mail-in, absentee, vote-by-mail> envelopes are returned to local election offices by the Postal Service. A manual review of the envelopes shows that several addresses are incomplete, incorrect, or the ballot is addressed to someone who does not live at that address.

A local media outlet, acting on a message from a resident, submits an inquiry to your office questioning the legitimacy of the ballots.

Day 55

A social media post from Hippoponymous encourages their followers to set up a "party at the box." Parties should have Hippoponymous logos and partygoers are encouraged to demonstrate against the Hippoponymous candidate's lack of representation on the ballots due to a failure to qualify.

Day 56

Voters using the 'Track Your Absentee Ballot' application on the Secretary of State (SOS) website don't see conformation that their ballots were received by the election office. Voters begin contacting their election office for a replacement ballot. Soon local county offices are sending out nearly as many replacement ballots as original ballots, and they begin to worry that they won't have enough ballots for polling places on election day.

One election official attempts to use the 'Track Your Absentee Ballot' feature on the <State> SOS website multiple times with information they are certain is in the system, but each query states that "no request is found associated with the information used." They report this to the State.

Discussion Questions

1. In relation to your organization's severity schema, what must occur for the incident response plan to be initiated?
    a. Describe what actions would be taken at this point in the scenario according to your organization's incident response plan.
    b. What training is conducted to familiarize your organization's employees with their roles and responsibilities in the incident response plan?
2. What internal and external intrusion detection capabilities/resources are available to alert and analyze inconsistencies on your network(s)?
3. How would your organization know which voter registration entries are valid?
4. How does your organization monitor activity in the statewide voter registration database?
5. What actions would you take based on the ballot addresses being incomplete or ballots being mailed to voters who have moved?
6. What are your procedures for handling misprinted ballots?
7. What are your public affairs concerns at this point in the scenario?
    a. What message would your organization communicate to the public?
8. What capabilities and resources are required to respond to the events in the scenario?
    a. What internal resources do you depend on and are they sufficient?
    b. Whom do you contact if you need additional third-party assistance?
    c. How are state and/or additional local resources requested?

Module 3

Day 57

A pallet of <mail-in, absentee, vote-by-mail> envelopes delivered to the election office was unintentionally damaged during transport. Some envelopes are postmarked prior to the <insert day of the week> before the election, but postmarks for many of the envelopes illegible. Additionally, your local post office representative contacts you stating that ballots have been found separated from their envelopes at several post offices.

Day 70 – Election Day – Morning

On Election Day, several < county, local municipality > websites have been altered with inaccurate information regarding drop box times and locations. The <State Chief Election Official's> website is also defaced with an image of the hashtag #Rigged20<XX>. IT staff at the state and the local jurisdictions are initially unable to fix the website.

Hippoponymous party protests surround drop boxes throughout the state. The protestors refuse to let voters return their ballots, claiming they are having a party. Media reports begin circulating about the parties at the drop boxes.

Day 70 – Election Day – Afternoon

The news media begins contacting both state and <county, local municipality> officials for comment regarding rumors of the vote tabulation system being hacked and social media allegations of election rigging.

Later in the afternoon, media outlets report that a ballot drop box at one of the Hippoponymous party locations caught on fire. The outlet reports that the ballots were completely destroyed.

Day 70 – Election Day - Evening

At <poll closing time> staff begin the process to close the <polls, voting period, etc.>. When local election office staff are about to transfer <the final set or final count of> vote totals to the state, multiple <county, local municipality > systems lock up and computer screens display a demand for a ransom of $50,000 to regain control of the infected devices. The vote totals are also encrypted and cannot be transferred.

Day 71

The day after the election, rumors begin to spread on social media regarding the election results. Voters are claiming that since some < county, local municipality > received multiple applications for an <mail-in, absentee, vote-by-mail> ballot, voters cast more than one ballot. Others claim that they were disenfranchised from voting because fewer polling places were available, and they were scared to vote due to protests.

Discussion Questions

1. What are your top priorities?
    a. How would these events affect the election processes?
    b. What systems would you prioritize for recovery?
2. What are your procedures when you receive damaged ballots?
    a. How often is this process reviewed/updated?

3. Do you have processes or procedures to address the damage to the ballot drop box or the potentially missing ballots?
4. What backup systems are used for ballots?
    a. How quickly can they be deployed?
    b. How often are backups created or updated?
5. What additional resources, if any, would your organization need to respond to the events presented in the scenario?
6. How would you collect evidence and maintain the chain of custody?
7. What is your public messaging?
    a. What pre-scripted messaging does your organization have?
    b. What organizations would you coordinate public messaging efforts with?
8. What ransomware policies and procedures are included in your incident response plan?
    a. What is the decision-making process to determine ransomware payment and who decides?
    b. What are the advantages/disadvantages to agreeing/refusing to pay?
    c. What are the political ramifications of this decision?
    d. What outside partners/entities do you need to contact?
9. How would you maintain the public's confidence in the election process given the events described in the scenario?

Appendix A: Additional Discussion Questions

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

Cyber Preparedness and Planning

1. How does your organization integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
2. Discuss your supply chain concerns related to cybersecurity.
3. How do you communicate your cybersecurity concerns to your vendors and how do you evaluate their cybersecurity performance?
4. What role does organizational leadership play in cybersecurity? Does this role differ during steady-state and incident response?
5. What level of funding and/or resources are devoted to cyber preparedness? Based on your risk assessment, what is the range of potential losses from a cyber incident?
6. Discuss cyber preparedness integration with your current all-hazards preparedness efforts. Who are your cyber preparedness stakeholders (public, private, non-profit, other)?
7. What mission essential functions depend on information technology and what are the cascading effects of their disruption?
8. Have you had any external review or audit of your IT plans, policies, or procedures within the last year?
9. How are background checks conducted for IT, security and key supporting personnel?
10. Which individual or department is in charge of cybersecurity management?
11. How does your organization recruit, develop, and retain cybersecurity staff?
12. How well-defined is cybersecurity in relation to contracts with third-party support vendors and crucial suppliers?
    a. How often are contracts reviewed?
    b. How well do your service level agreements address incident response?
13. Discuss the status of cyber preparedness planning within your organization.
    a. Have you completed a business impact analysis? Does the analysis include information technology (IT) infrastructure supporting mission essential functions identified in continuity of operations and continuity of government plans?
    b. How is cybersecurity integrated in your business continuity plans? Does your business continuity and/or disaster recovery planning have a prioritized list of information technology infrastructure for restoration?
    c. How have IT specific plans been coordinated with other planning efforts such as an Emergency Operations Plan or Continuity of Operations Plan?
14. How is cybersecurity integrated into both organizational and project risk assessments and management?
15. How does your organization implement a formal sanctions process for personnel failing to comply with established information security policies and procedures? Has this process been communicated to employees?

16. Does your organization have a cybersecurity incident response plan? When was it issued? When was the incident response plan last revised? What authorities require which departments or agencies to follow the plan?
17. Does your organization utilize multi-factor authentication?
18. Does your IT department have a patch management plan in place? If so,
    a. Are risk assessments performed on all servers on the network?
    b. Are processes in place to proactively evaluate each server's criticality and applicability to software patches?
    c. Does this plan include a risk management strategy that addresses the following considerations?
        i. The risks of not patching reported vulnerabilities?
        ii. Extended downtime?
        iii. Impaired functionality?
        iv. The loss of data?
19. What is your method for tracking and/or identifying problematic pieces of firmware in your organization, should a vulnerability be identified?
20. What processes does your organization have in place for when an employee is terminated or resigns?
    a. What additional processes are implemented if the employee's termination is contentious?
    b. How does your organization retrieve all information system-related property (e.g., authentication key, system administration's handbook/manual, keys, identification cards, etc.) during the employment termination process?
21. What protections do you have in place to protect against malicious intent by those vendors or outside parties that have access to your network?
    a. What access does any of your third-party vendors have into your network?
22. What are your identified responsibilities for, and capabilities to, prevent cyber incidents?
23. Who is responsible for network and information security management?
24. What key documents that support cyber preparedness at a federal, state, or local level can you identify?
25. Does your organization follow a cybersecurity standard of practice (NIST Cybersecurity Framework/800 Series, ISO/IEC, etc.)? If so, which?
26. What flowcharts showing the high-level relationships and crisis lines of communication (i.e., who calls who) specifically for a cyber incident does your organization have? Are they part of the response or continuity planning documents?
27. What is your organization's formal or informal policy or procedures pertaining to IT account management?
    a. Do these policies or procedures include protocols for establishing, activating, modifying, disabling, and removing accounts?
    b. Do these policies or procedures include protocols/steps for notifying IT account managers/administrators when users are terminated?
28. How are IT and business continuity functions coordinated with physical security? How do IT, business continuity, and physical security components collaborate with your public relations, human resources, and legal departments?

29. What processes do you have to ensure that your external dependencies (contractors, power, water, etc.) are integrated into your security and continuity planning and programs?
30. Describe the decision-making process for protective actions in a cyber incident. What options are available? Have these options been documented in plans? How are they activated?
31. What immediate protective and mitigation actions would be taken at your organization in this scenario? Who is responsible for those actions?
32. What protective actions would you take across non-impacted systems or agencies in the scenario presented? Who is responsible for protective action decision-making? How are actions coordinated across parts of the organization?
33. Compare and contrast physical and cyber incident notifications and protective action decision-making.
34. What systems or processes are the most critical to running elections?
    a. How are these systems or processes codified in your incident response plan?
    b. What processes are in place to run elections in the event computer systems are compromised?
35. How do you protect the integrity of your voter registration database?
    a. What entities have access to the database?
    b. How would those entities report a breach of their systems to your office?
36. How do you protect the integrity of your voting equipment?
    a. What entities have access to your <state, county, local> voting equipment?
    b. What entity is responsible for securing the voting equipment?
    c. Does your organization maintain contact information with all relevant parties in case of an incident?
37. What is your planned cyber incident management structure?
    a. Who (by department and position) leads incident management and why?
    b. How are they notified?
    c. When did they last exercise their role?
    d. What is the length of your operational period (i.e., your "battle rhythm")?
38. What are the primary and contingency communication mechanisms necessary to support incident management?

Information Sharing

1. How would your organization receive the information presented in the scenario?
    a. Through what channels would this information be received and disseminated?
    b. What are your established mechanisms to facilitate rapid information dissemination?
    c. What are your known communication gaps? Who in your organization is responsible for addressing those gaps?
    d. What actions, if any, would your organization take based on this information?
2. What sources of cybersecurity threat intelligence does your organization receive? For example, information from the Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), open source reporting, security service providers, others?
    a. What cyber threat information is most useful?
    b. How timely and actionable is the information that you receive?

   c. Who is responsible for collating information across the organization?

3. What mechanisms and products are used to share cyber threat information within your organization and external to your organization (e.g., distribution lists, information sharing portals)?
4. Describe how variables in threat information (timeframe, credibility, and specificity) impact decision-making.
5. How do local government entities report information to state partners?
6. What information, if any, would be shared between the local government IT offices, local election officials, and state officials?
   a. How would this information be shared and is this process documented and/or formalized?
7. How is information shared among your internal and external stakeholders? Through formal or informal relationships? What information sharing mechanisms are in place?
8. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing? Is information flowing in both directions?

Incident Identification

1. How do employees report suspected phishing attempts?
   a. What actions does your department take when suspicious emails are reported?
   b. Are there formal policies or plans that would be followed?
   c. Does your department conduct phishing self-assessments?
2. What process does the general workforce follow to report suspected cyber incidents? Is this a formal process on which they have been trained?
3. What would cause you or someone in your organization to report a cybersecurity incident?
   a. How are incidents reported?
   b. What would trigger the reporting requirements established by State law and policy?
   c. Who has the authority to create and enforce cybersecurity policies in your organization?
   d. What training have employees received regarding your cyber incident response plan?
4. What cybersecurity incident escalation criteria, notifications, activations, and/or courses of action are defined in your response plan?
   a. Who would be responsible and what actions would they take?
   b. How and when would your leadership be notified?
5. How does your organization baseline network activity? How would you be able to distinguish between normal and abnormal traffic?
6. How does the organization report cybersecurity incidents to outside organizations? To whom? What, if any, mandatory reporting requirements do you have?
7. How do detection and analysis procedures differ for loss of personally identifiable information (PII), phishing attempts, data exfiltration, data modification, or other incidents?
8. Who is responsible for correlating information across different organizational-level incidents?
9. Discuss your organization's intrusion detection capabilities and analytics that alert you to a cyber incident.

10. What type of hardware and/or software does your organization use to detect/prevent malicious activity of unknown origin on your systems/network?
11. What is your organization's primary concern at this time?
12. What Day, if any, would prompt you or someone in your organization to report a cybersecurity incident?
    a. How would reports flow between different levels of government (e.g., local reporting to state, or state to federal)?
13. Do you have someone within your organization who monitors the Dark Web? If so, how would you verify the security researcher's claims and confirm authenticity of the sensitive information in question?

Incident Response

1. What level of leadership/management would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?
2. What is your department or agency's primary concern? Mitigation of the incident (resolving the issue) or investigation (preserving the evidence to build a criminal case)? Who would make this decision? Are these mutually exclusive?
3. What response actions would your organization have taken at this point? Are these actions driven by a plan?
4. What impact will the sale of sensitive or Personally Identifiable Information (PII) have on your response and recovery activities?
    a. Will it alter priorities? Have your public relations priorities changed?
    b. Will it trigger any additional legal or regulatory notifications?
5. Whom will you notify, internally and externally, of these incidents?
    a. Is there a process or plan in place that outlines the severity thresholds for which different notifications are made and what information is to be conveyed?
    b. How will you keep senior leadership updated? What information is provided and how is it communicated?
    c. How and when would you make a notification to the public?
        i. How are you coordinating your messaging within your organization?
        ii. What pre-canned messaging or holding statements does your organization have for such an event?
    d. How are you ensuring unity of message between your organization, the public sector, and elected officials?
6. How would these events affect your organization's business operation/processes?
7. What concerns have these incidents generated that have not been addressed?
8. How would your organization respond to the discovery of a malicious, unauthorized administrator account on your systems? Who would be informed internally? Who would be informed externally (e.g., law enforcement, cybersecurity insurance partners, etc.)?
9. What resources are required for incident investigation and attribution? Are sufficient resources available in-house?

10. How would the events presented in the scenario trigger activation of your cyber incident response plan or similar document (e.g., emergency operations plan cyber incident annex)? How would the activation alter any roles and responsibilities?
11. At what point in the scenario would you contact law enforcement and/or the state Attorney General?
    a. How would relationships with law enforcement and other partners be managed? Where is the process documented?
    b. How does a law enforcement investigation impact containment, eradication, and recovery efforts?
    c. What processes and resources are in place for evidence preservation and collection?
12. Discuss the difference between network and host forensics. How are you equipped and staffed to address this?
13. What are the roles of your network operations center and security operations center during a response?
14. What are your essential elements of information and key information questions necessary for operational and executive-level responses to cyber incidents?
15. What mission essential functions are impacted by the incidents described in the scenario?
16. How does your organization maintain service availability of key assets (e.g., network connectivity, etc.)?
17. What capabilities and resources are required for responding to this series of incidents?
    a. What internal resources do you depend on? Are your current resources sufficient?
    b. Whom do you contact if you're in need of additional third-party assistance?
    c. What resources are available within the state or locally? How do you request these resources?
    d. Do you have personnel tasked with incident response or a designated cyber incident response team within your organization?
        i. If so, what threshold must be reached for the cyber incident response personnel to be activated? Does this scenario reach that threshold?
        ii. Who is responsible for activating the cyber incident response personnel and under what circumstances?
        iii. What are the cyber incident response team/personnel's roles and responsibilities?
18. In what ways, if any, does this scenario exceed your organization's ability to respond?
    a. What are your organization's established procedures to request additional support?
19. What are your organization's response priorities?
    a. Who would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?
    b. What response actions would the IT/IS department take at this point? Are these actions driven by a plan?
    c. What response capabilities and resources are required to respond to these incidents?
20. What actions would be taken when the exfiltration is discovered? Does your organization have written plans that would be implemented?
21. What is the decision process to determine if the ransom should be paid or not?

   a. Who decides?
   b. What is the process?
   c. What are the advantages/disadvantages?
   d. What are the political ramifications?
   e. What outside partners/entities do you need to contact?

22. Where do you receive cyber response technical assistance? What plans, procedures or policies are in place to access this assistance?
23. How does your organization proactively identify and establish the service provider relationships needed for incident/breach response issues (e.g., credit counseling, forensic/computer security services)?
24. What processes are used to contact critical personnel at any time, day or night?
    a. How do you proceed if critical personnel are unreachable or unavailable?
25. If your pollbook or other critical election information system were disabled, how would you continue elections operations?
    a. What, if any, additional resources would you need to conduct elections if your elections information was unrecoverable?
    b. Do you have mechanisms in place (e.g., MOU/MOA, contract, etc.) for arranging additional surge support of both personnel and resources on Election Day, should it be needed?
26. How would your organization respond to misprinted <ballots, envelopes, or other printed election materials>?
27. How would a breach of another agency affect the <your entity> if they potentially have access to your information?
    a. Is the agency required to notify <your entity> of their breach or suspected breach? If so, what are the notice requirements?
28. Given the events of <Election Day, early voting> what is your greatest priority?
29. If the networks were found to be infected with ransomware, how would this impact the certification of election results?
    a. If election results from your <precinct, municipality, county> cannot be certified, how would you proceed?
30. How would voters locate their <polling location> if the locator were vandalized or disabled?
31. How would you determine whether unauthorized manipulation of election data has occurred?
    a. How would you address the absence or alteration of voter data in the pollbooks?
    b. How would you reconcile a greater number of voters versus available voters registered?
32. How would you respond to the allegations that the election <data, results, or other assets> were damaged or destroyed?
    a. What partners would you involve in the response?
    b. Have you drafted messaging in advance of an incident?
33. If primary communications are compromised, how do you provide information to internal and external entities?
34. What actions, if any, would you take based on the ballot addresses being incomplete or ballots being mailed to voters who have moved?

35. How would you handle the misprinted ballots?
36. How are voters able to vote in the event the voter registration database is compromised?
37. In the event of complete failure of your entity's general network or election network, what systems would you need to successfully run an election?
38. How would you respond to the attempts to discredit the elections process on social media?

Recovery

1. When does your organization determine a cyber incident is closed?
    a. Who makes this decision?
    b. Would your organization engage in any post-incident activities?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
    a. Would senior leaders consider re-activating critical business processes and systems? What is the risk associated with doing so?
    b. Would your organization consider a complete rebuild of these systems? How long and costly would that process be?
    c. What factors do you consider when making these decisions?
3. What formal policies and procedures does your organization use to decide when and how to restore backed-up data, including measures for ensuring the integrity of backed-up data before restoration?
4. Does your organization have back-ups of vital records (e.g., the voter registration database, etc.) in a location that is separated from your primary working copies of your files?
    a. How frequently do you run backups?
    b. How long do you keep any copies of archived files backed up?
    c. How long of a downtime would exist between your primary files and the restoration of files via your back-up?
5. What redundant systems are in place if the impacted system(s) is compromised?
    a. What alternative systems or manual processes are in place to continue operations if a critical system is unavailable for a significant period of time?
    b. Who can authorize use of alternate systems or procedures?
6. What backup systems are utilized in your organization?
    a. How quickly can they be deployed?
    b. How often are backups created or destroyed?
7. Describe your role in post-incident activity.
8. How would you work with critical infrastructure providers to determine the incident is over?
9. How does post incident-activity differ when critical infrastructure is involved?
10. Does your organization have a continuity of operations plan (COOP) for conducting its functions at a location other than your main building?
    a. If so, how would a suspected cyber incursion impact your organization's ability to activate its COOP Plan?
11. What further concerns do you have that have not been discussed?

Training and Exercises

1. What basic cybersecurity and/or IT security awareness training does your organization provide to all users (including managers and senior executives)?
    a. How often is training provided?
    b. What topics are covered in your training?
    c. Is training required to obtain network access?
    d. What security-related training does your department or agency provide to, or contractually require of, IT personnel and vendors with access to your city's or county's information systems? How often do they receive the training?
2. How does your organization train elections personnel, including volunteers, on cybersecurity threats such as phishing?
    a. How often is training provided?
    b. What topics are covered in the training sessions?
3. What special training, if any, do your cybersecurity incident response team members undergo to detect, analyze, and report this activity? Describe this training.
    a. How is your staff trained to read and analyze your intrusion detection system logs?
4. What training do you provide in support of your Cybersecurity Incident Response Plan, Business Continuity Plan, Emergency Operations Plan Cyber Incident Plan, or other related plans?
    a. Do employees know what constitutes suspicious cybersecurity activities or incidents?
    b. Do employees know what actions to take when one arises?
5. If you have a cyber incident response plan, how often does your organization exercise the plan?
    a. Who is responsible for the exercise planning?
    b. What agencies are involved in the exercise?
    c. What level of the organization is required to participate?
    d. What actions follow the exercise?
6. What are your cybersecurity incident response team's exercise requirements?
7. How does your organization's efforts address both physical and cyber risks?
8. Have senior or elected officials participated in a cybersecurity exercise?
9. What are the additional training and/or exercising requirements for your organization?

Senior Leaders and Elected Officials

1. What is your cybersecurity culture? As a leader in your organization, what cybersecurity goals have you set? How have they been communicated?
2. As it relates to your jurisdiction, what cybersecurity information do you request? What do you receive?
3. What are your cybersecurity risks?
4. Who develops your jurisdiction's cybersecurity risk profile? What are their reporting requirements? Are they directed to, required by statute, or other? How often do they report?
5. How is your cybersecurity risk integrated with physical risk for an integrated jurisdictional risk assessment?

6. What is your jurisdiction's greatest cybersecurity concern? Why do you rate this concern as your greatest concern? Who reports to you on cyber threats?
7. What, if any, infrastructure does your jurisdiction own, operate, and/or regulate?
8. What relationships do you have with critical infrastructure owners and operators?
9. What priorities have you set related to the cybersecurity of critical infrastructure?
10. What is your most important critical infrastructure?
11. What are your regulatory requirements related to critical infrastructure, if any?
12. What is the greatest threat facing your critical infrastructure? What, if anything, is your jurisdiction able to do to mitigate it?
13. When did you last receive a cyber threat briefing for your jurisdiction?
14. How has your jurisdiction prepared for a cyber incident? Does your jurisdiction have cybersecurity plans in place? How many information security officers do you have? Does the plan indicate how they will work together?
15. Have your information security officers and emergency managers jointly planned for cybersecurity incidents?
16. What are your cybersecurity workforce gaps? How does your jurisdiction recruit, develop, and retain cybersecurity staff?
17. What cybersecurity training do you have planned for cybersecurity staff, managers, and general workforce?
18. What magnitude of incident would require you be notified? How does that notification process work? Is it planned?
19. What requirements or agreements, if any, exist for critical infrastructure to notify you of a cyber incident?
20. Who advises you on cyber threats? What are your essential elements of information or critical information requirements?
21. What is your planned role in protective action decision-making?
22. What is your planned cyber incident management structure? What parts of the government need to be engaged?
23. Would your jurisdiction's Emergency Operations Center be activated in a cyber incident? How? Why?
24. What is your role in a cyber incident?
25. How does a law enforcement investigation impact your response?
26. What is your role in communicating to the public?
27. How are costs of the response calculated?
28. What information do you need to support your decision-making process?
29. Who is your jurisdiction's cybersecurity liaison to privately-owned and operated critical infrastructure?
30. What are your expectations of the State and Federal Government?
31. Describe your role in post-incident activity.
32. What is your role in restoring and/or maintaining public confidence?

Public Affairs

1. What are your public affairs concerns? Who is responsible for coordinating the public message? Is this process a part of any established plan?
    a. How would your department respond to the local media reports?
    b. What information are you sharing with citizens? Employees?
    c. Are public information personnel trained to manage messaging related to cyber incidents?
    d. Does your department have pre-drafted statements in place to respond to media outlets?
    e. Are they trained to manage your social media presence?
    f. Are all personnel trained to report any contact with the media to appropriate public information personnel?
2. What information would your organization communicate to the public? How would you communicate it?
3. Who is responsible for public information related to the incident? What training or preparation have they received?
4. How would your organization respond to the attempts at disinformation/misinformation concerning elections?
    a. What established public messaging processes does your organization have as part of a larger communications plan?
    b. How would your organization respond to the social media posts/rumors and local media reports? Would you use social media or respond by drafting statements?
    c. What message are you sending employees?
    d. How are personnel trained to report any contact with the media to the appropriate public information personnel?
5. How would you inform other entities of the fake websites and social media pages?
    a. How would you contact social media platforms?
    b. What issues or challenges have you had in working with them?
6. How would your organization respond to the emerging news and social media issues?
    a. Does your organization have pre-approved messages for immediate release as part of a larger communications plan?
7. What steps are you taking before an incident to build relationships with the media and with voters before an incident happens?

Legal

1. What are the legal issues you must address?
2. What policies should your organization have? Does it exercise these policies? If so, how often?
3. What legal documents should your organization have in place (for example with third-party vendors)?
4. What is the role of the legal department in this scenario?
5. What security breach notification laws does your state have? What do these laws include?
6. What are the consequences if you are unable to certify the official election results?
7. What processes are in place to collect evidence and maintain the chain of custody?

Appendix B: Acronyms

Acronym	Definition
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
DDoS	Distributed Denial of Service
EI-ISAC	Elections Infrastructure Information Sharing and Analysis Center
FBI	Federal Bureau of Investigation
IT	Information Technology
IoT	Internet of Things
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
SOS	Secretary of State
TLP	Traffic Light Protocol

Appendix C: Case Studies

Emotet Malware Infection

On the morning of March 1, 2020, the city of Torrance, California, fell victim to a cyberattack. Servers were impacted, causing interruptions in computer access to several departments throughout the city. Access to email was lost, credit cards couldn't be processed, and the website completely lost its functionality. Employees had to use temporary email accounts to perform some of their core job functions. The attack caused a major disruption and took many hours to get systems back up and running. Although the attackers were able to take down the city's systems, it's believed that no personal data were compromised during this incident. Torrance did not disclose whether a ransom had been demanded by the attackers.[1]

On August 11 and 12, 2020 the Department of Justice of Quebec suffered a cyberattack in which threat actors used malicious software to compromise 14 inboxes under the Department jurisdiction. The attackers gained access the emails addressed to these mailboxes. The hackers used a version of the Emotet malware. In this case the hackers used the stolen information to spread their malware. Cybercriminals sent seemingly legitimate messages to those who contacted the afflicted mailboxes, appearing to originate from the Department, and included malicious attachments. Officials stated, "the hackers allegedly stole the personal information of approximately 300 active and inactive employees (retired or now working elsewhere)."[2]

Distributed Denial of Service Attack

Elections officials across the country have been working to harden their systems against DDoS and other attacks since 2016. The days just before and after Election Day are the most likely time for adversaries to launch DDoS attacks.[3] Beyond voter information portals and registration sites that give voters information about voting hours or where they can vote, prime DDoS targets include election night results websites and communications between boards of elections and polling locations.[4] According to CISA and the FBI, while attacks on election infrastructure can hinder access to voting information, "the underlying data and internal systems would remain uncompromised, and anyone eligible to vote would still be able to cast a vote.[5]"

---

[1] *"The Top Cyberattacks of March 2020"*. (April 8, 2020). Retrieved February 25, 2021 from Artic Wolf: https://arcticwolf.com/resources/blog/the-top-cyberattacks-of-march-2020

[2] *"Emotet strikes Quebec's Department of Justice: An ESET Analysis"*. (September 16, 2020). Retrieved February 25, 2021 from WeLiveSecurity: https://www.welivesecurity.com/2020/09/16/emotet-quebec-department-justice-eset/

[3] Starks, Tim, "The lowly DDoS attack is still a viable threat for undermining elections." *Scoop News Group*, October 27, 2020. Accessed March 3, 2021. https://www.cyberscoop.com/lowly-ddos-attack-still-viable-threat-undermining-elections/

[4] Ibid.

[5] FBI & CISA, "DDoS Attacks on Election Infrastructure Can Hinder Access to Voting Information, Would Not Prevent Voting." *Public Service Announcement*, September 30, 2020. Accessed March 3, 2021. https://www.cisa.gov/sites/default/files/publications/PSA_DDoS_Final%20-%20CyD_508pobs.pdf

In May 2018, the website used to display voting results for the Knox County, Tennessee mayoral primary was taken offline by a DDoS. This prevented voters from being able to access the site and view the results of the primary, but voting tallies were not affected by the attack.[6] According to preliminary analysis of the DDOS attack by Knox County's IT Director Dick Moran, the attack was "extremely heavy and abnormal network traffic was originating from numerous IP addresses associated with numerous geographic locations, both internal and external to this country.[7]" Further investigation determined that the DDoS was a smokescreen to distract the county while another, simultaneous attack was happening behind the scenes accessing county information.[8]

Social Engineering

Attacks were launched against a certain customer base that claimed to be from a violent hate group, directing recipients to vote for a certain candidate in the 2020 election. The attacker had access to the recipient's personal information as well as the ability to identify how the recipient typically votes. This sort of intimidation-based social engineering was similar to strategies seen in extortion attacks. The attacker has some amount of personal information about the recipient, such as their name or address, acquired through data leaks or publicly. In addition, the attackers indicated they had access to something even more concerning, such as a compromising video or a bomb placed at a school or place of business. The sources were mainly compromised mail infrastructure; the only way to identify these messages was through content understanding.[9]

One notorious Arizona voter registration 'error' phishing scam informs recipients that their voter's registration applications are incomplete, luring them into sharing Social Security numbers, license data and other personal information with attackers. The fraudulent emails sent in this campaign appear to come from the U.S. Election Assistance Commission, and contain a malicious URL leading to a spoofed web page that steals a variety of personal data including name, date of birth, mailing address, email address, Social Security number and driver's license information. The page is carefully engineered to appear legitimate, and even includes images pulled from ServiceArizona's official site.[10]

Ransomware

In October 2020, a U.S. state county was hit with a ransomware attack on their county and election infrastructure. The attack affected the county's voter signature database, as well as the voting

---

[6] Abrams, Lawrence, "Knox County Tennessee Election Site Hit with DDOS Attack During Primary." *Bleeping Computer,* May 5, 2018. Accessed March 3, 2021. https://www.bleepingcomputer.com/news/security/knox-county-tennessee-election-site-hit-with-ddos-attack-during-primary/

[7] Ibid.

[8] Whetstone, Tyler, "Knox County election night cyberattack was smokescreen for another attack." *Knox News,* May 17, 2018. Accessed March 3, 2021. https://www.knoxnews.com/story/news/local/2018/05/17/knox-county-election-cyberattack-smokescreen-another-attack/620921002/

[9] Day, B. (2020). FBI: The 2020 Presidential Election Is Under Attack by Email Scammers. *Digital Guardian,* October 19, 2020, Retrieved March 1, 2020 from https://guardiandigital.com/blog/fbi-the-2020-presidential-election-is-under-attack-by-email-scammers

[10] Author Unknown (2020). Election Interference & Social Engineering, (2020, October 23). *Abnormal Security*. Retrieved March 1, 2021 from https://abnormalsecurity.com/blog/election-interference/

precinct map hosted on the county website. In this case, attackers did not specifically target election systems, but the loss of access to the voter signature database significantly slowed down absentee ballot processing. County officials were still able to verify voter signatures using paper copies of voter registration cards and the voting process was not impacted by the ransomware attack. State election infrastructure systems were also unaffected. However, the attack raised concerns regarding the potential impacts of ransomware on election infrastructure systems.[11]

In September 2020, a U.S. company that sells election results software to cities and states was hit by ransomware. While the company is not responsible for tallying votes, the software is used by election officials to aggregate and report votes in at least 20 locations around the US. The attack initially appeared to be a routine ransomware attack where the company's data was encrypted, but it was later reported that several of the company's clients witnessed unauthorized individuals trying to access their systems. The company launched an investigation into the attack and ultimately paid an undisclosed ransom amount to unlock their systems.[12]

[11] Reed, Megan, "How Hall County is Handling Influx of Absentee Voting, Effects of Ransomware Attack on Elections Office." *The Gainsville Times*, October 23, 2020. Accessed 23 February 2021, https://www.gainesvilletimes.com/news/politics/how-hall-county-handling-influx-absentee-ballots/; Forno, Richard, "Ransomware Can Interfere with Elections and Fuel Disinformation – Basic Cybersecurity Precautions Are Key to Minimizing the Damage." *Government Technology,* October 30, 2020. Accessed 23 February 2021, https://www.govtech.com/security/Ransomware-Can-Interfere-with-Elections-and-Fuel-Disinformation--Basic-Cybersecurity-Precautions-Are-Key-to-Minimizing-the-Damage.html

[12] Perlroth, Nicole and David E. Sanger, "Ransomware Attacks Take on New Urgency Ahead of Vote." *The New York Times*, September 27, 2020. Accessed 23 February 2021, https://www.nytimes.com/2020/09/27/technology/2020-election-security-threats.html; Johnson, O'Ryan, "Tyler Technologies Reportedly Paid Ransomware, Like Many Other Victims, Expert Says." *CRN,* October 12, 2020. Accessed 23 February 2021, https://www.crn.com/news/channel-programs/tyler-technologies-reportedly-paid-ransomware-like-many-other-victims-expert-says

Appendix D: Attacks and Facts

Distributed Denial of Service

Distributed Denial of Service (DDoS) attacks overload bandwidth and connection limits of hosts or networking equipment, specifically through a network of computers making excessive connection requests. DDoS attacks unfold in stages. First, a malicious actor infects a computer with malware that spreads across a network. This infected computer is known as the "master" because it controls any subsequent computers that become infected. The other infected computers carry out the actual attack and are known as "daemons." The attack begins when the master computer sends a command to the daemons, which includes the address of the target. Large numbers of data packets are sent to this address, where extremely high volumes (floods) of data slow down web server performance and prevent acceptance of legitimate network traffic. The cost of a DDoS attack can pose sever loss of revenue or reputation to the victim.

More information on DDoS attack possibilities within each layer of the OSI Model, as well as traffic types and mitigation strategies, can be found in the resource list below.

Additional Resources

- Understanding Denial-of-Service Attacks (https://www.us-cert.gov/ncas/tips/ST04-015)
- DDoS Quick Guide (https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf)
- Guide to DDoS Attacks (https://www.cisecurity.org/wp-content/uploads/2017/03/Guide-to-DDoS-Attacks-November-2017.pdf)

Social Engineering

One of the most prominent tactics attackers 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. 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, evading intrusion detection systems without leaving a log trail, and is completely operating system platform dependent. 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, know where to forward them and keeping software and systems up-to-date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.us-cert.gov/ncas/tips/ST04-014)
- The Most Common Social Engineering Attacks (https://resources.infosecinstitute.com/common-social-engineering-attacks/)

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. 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 Ransomware (www.stopransomware.gov)
- Protecting Against Ransomware (https://www.us-cert.gov/ncas/tips/ST19-001)
- Indicators Associated with WannaCry Ransomware (https://www.us-cert.gov/ncas/alerts/TA17-132A)
- Incident trends report (Ransomware) (https://www.ncsc.gov.uk/report/incident-trends-report#ransomware)

Appendix E: Doctrine and Resources

Laws

- National Cybersecurity Protection Act of 2014 (Dec 2014) https://www.congress.gov/113/plaws/publ282/PLAW-113publ282.pdf
- Federal Information Security Modernization Act of 2014 (Dec 2014) https://www.dhs.gov/fisma
- OMB Memorandum: M-15-01, Fiscal Year 2014-2015: Guidance on Improving Federal Information Security and Privacy Management Practices (Oct 2014) https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf

Presidential Directives

- Executive Order 13800: Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure (May 2017) https://www.whitehouse.gov/presidential-actions/presidential-executive-order-strengthening-cybersecurity-federal-networks-critical-infrastructure/
- Presidential Policy Directive-41: United States Cyber Incident Coordination (Jul 2016) https://obamawhitehouse.archives.gov/the-press-office/2016/07/26/presidential-policy-directive-united-states-cyber-incident
- Annex to Presidential Policy Directive-41: Annex to the Directive on United States Cyber Incident Coordination (Jul 2016) https://www.hsdl.org/?view&did=797545
- Presidential Policy Directive-8: National Preparedness (Mar 2011), (Updated Sep 2015) https://www.dhs.gov/presidential-policy-directive-8-national-preparedness
- Presidential Policy Directive 21: Critical Infrastructure Security and Resilience (Feb 2013) https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil
- Executive Order 13636: Improving Critical Infrastructure Cybersecurity (Feb 2013) https://www.hsdl.org/?view&did=731040

Strategies and Frameworks

- National Cyber Incident Response Plan (Dec 2016) https://www.us-cert.gov/ncirp
- National Cyber Strategy of the United States of America (Sep 2018) https://www.whitehouse.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf
- U.S Department of Homeland Security Cybersecurity Strategy (May 2018) https://www.hsdl.org/?view&did=810462
- Framework for Improving Critical Infrastructure Cybersecurity (Apr 2018) https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf
- National Protection Framework, Second Edition (Jun 2016) https://www.fema.gov/media-library-data/1466017309052-85051ed62fe595d4ad026edf4d85541e/National_Protection_Framework2nd.pdf
- Office of Management and Budget (OMB) Memorandum: M-16-04, Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government (Oct 2015) http://www.thecre.com/forum4/wp-content/uploads/2015/11/OMB-Cybersecurity-Implementation-Plan.pdf

Key Points of Contact

- Cybersecurity and Infrastructure Security Agency (CISA) (contact: central@cisa.dhs.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)
- National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; (855) 292-3937)
- United States Secret Service Field Offices and Electronic Crimes Task Force (ECTFs) (contact: https://www.secretservice.gov/contact/field-offices/)

Other Available Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; (518) 266-3460)
- Cybersecurity and the States (National Association of State Chief Information Officers [NASCIO]) (http://www.nascio.org/Advocacy/Cybersecurity)
- National Governors Association (NGA) (https://www.nga.org/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- InfraGard (https://www.infragard.org/)
- Internet Security Alliance (http://www.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; contact: operations@certifiedisao.org)
- National Council of ISACs (https://www.nationalisacs.org/)

References Cited

"Wannacry Two Years Later: How Did We Get The Data?". (2019, Nay 27). Retrieved August 22, 2019, from Armis IOT Security: ttps://go.armis.com/hubfs/Armis-WannaCry-How-Did-We-Get-The-Data-WP.pdf

CISA. (2018, July). *Alert (TA18-201A) - Emotet Malware*. Retrieved from us-cert.gov.

Davis, J. (2018, 31 July). *1.4 million patient records breached in UnityPoint Health phishing attack*. Retrieved July 2019, from HealthCare IT News: ttps://www.healthcareitnews.com/news/14-million-patient-records-breached-unitypoint-health-phishing-attack

Davis, J. (2019, April 11). *Minnesota DHS Reports Health Data Breach from 2018 Email Hack*. Retrieved 2019, from Health IT Security: https://healthitsecurity.com/news/minnesota-dhs-reports-health-data-breach-from-2018-email-hack

Kottler, S. (2018, March 1). *February 28th DDoS Incident Report*. Retrieved 2019, from The GitHub Blog: https://github.blog/2018-03-01-ddos-incident-report/

Palo Alto Networks. (2019, February 2). *PAN-OS 8.0: PAN-OS Phishing Attack Prevention*. Retrieved July 2019, from Palo Alto Networks Knowledge Base: https://knowledgebase.paloaltonetworks.com/KCSArticleDetail?id=kA10g000000ClRpCAK

Seri, B. (n.d.). *"Two Years In and WannaCry is Still Unmanageable"*. Retrieved August 22, 2019, from Armis IOT Security Blog: https://www.armis.com/resources/iot-security-blog/wannacry/

Sullivan, P. (2018, July 31). *Mat-Su Declares Disaster for Cyber Attack*. Retrieved July 2019, from Matanuska-Susitna Borough: https://www.matsugov.us/news/mat-su-declares-disaster-from-cyber-attack

Symantec Threat Intelligence. (2017, October 23). *What you need to know about the WannaCry Ransomware*. Retrieved 2019, from Symantec Threat Intelligence Blog: https://www.symantec.com/blogs/threat-intelligence/wannacry-ransomware-attack