[Enter Organization Name]

CISA Tabletop Exercise Package

Local Governments

<Exercise Date>

<Exercise Title>
Situation Manual

Table of Contents

DISCLAIMER: This report is provided "as is" for informational purposes only. The Cybersecurity and Infrastructure Security Agency (CISA) does not provide any warranties of any kind regarding any information within. CISA does not endorse any commercial product or service referenced in this advisory or otherwise. This document is distributed as TLP:WHITE: Limited disclosure, restricted to participants' organizations. Recipients may only share TLP:WHITE 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. Sources are at liberty to specify additional intended limits of the sharing: these must be adhered to. For more information on the Traffic Light Protocol, see https://www.cisa.gov/tlp.

Handling Instructions

Delete instructions that are not applicable.

TLP: WHITE

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):WHITE*": Disclosure is not limited. Sources may use TLP:WHITE 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:WHITE information may be distributed without restriction.**

This document may be disseminated publicly pursuant to TLP:WHITE 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*" This designation is used 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. **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
	Time	Activity
	Time	Activity
Scope	X hour facilitated, discussion-based tabletop exercise.	
Purpose	Examine <insert your local government>'s ability to protect, detect, and respond to a disruptive cyber incident.	
INSERT: <NIST, FEMA, or Mission Capabilities>	For example, areas such as Identify, Protect, Respond, etc.	
Objectives	1. Assess <insert your local government>'s preparedness to mitigate and respond to cybersecurity incidents. 2. Examine the policies and procedures of <insert your local government>'s cyber incident response plan. 3. Discuss <insert your local government >'s internal and external communication processes and plans to address cyber incidents. 4. Explore <insert your local government >'s organizational information sharing, awareness, and cybersecurity posture.	
Threat or Hazard	Cyber	
Scenario	A threat actor targets <insert your local government>'s employees through a phishing email as an entry point into networks/systems. Attackers compromise workstations and data using ransomware with a payment deadline of 72-hours during which various cyber incidents occur.	
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	**CISA National Cyber Exercise Program (NCEP)** 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 addresses the types of cyber security alerts that your organization may receive along with your organization's cyber preparedness
  - **Module 2:** This module includes cybersecurity incidents that could impact not only your organization but other facilities in your area
  - **Module 3:** This module introduces cascading impacts of the cybersecurity incident on your organization and the response from residents and media in your local area
- 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 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

Employees from the < your local government>'s <Treasurer's Office> receives an email from Human Resources (HR) about new benefits for fiscal year <20XX>. The email instructs the user to sign the document and send it back to HR by close of business to ensure there is no lapse in benefits.

Some employees follow the instructions and submit their information, while others report the email to the <Information Technology (IT) department/help desk> as suspicious.

Day 4

The Cybersecurity and Infrastructure Security Agency (CISA) releases an alert regarding phishing campaigns targeting state, local, tribal, and territorial (SLTT) government networks. The phishing emails mention required updates to important HR documents and contain a malicious attachment that automatically installs ransomware. After gaining access to the network, threat actors escalate privileges for administrator rights without victims' action or authorization.

Day 5

The <your local government>'s IT department sends a message stating that they have received reports of an email that may be a part of a phishing campaign and to immediately report any suspicious emails.

Day 7

The <your local government>'s IT department notices unusual traffic to an external IP address over a HTTP port leaving HR's payroll servers. IT staff begin to investigate the anomaly, but it occurs only for a few minutes and stops, so they assume it was a one-time issue that has been resolved.

Discussion Questions

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

1. What cybersecurity threat intelligence does your organization receive?
   a. What plans and processes does your organization follow in the case of a cybersecurity alert like the one presented in this scenario?
   b. What actions would your organization take based on this information?
2. Describe your organization's cybersecurity training program for employees.
   a. How often are employees required to go through this training?
   b. What are the ramifications for employees not completing cybersecurity training?
   c. What additional training is required for employees who have system administrator-level privileges?
3. How do employees report suspected phishing attempts and/or other cybersecurity incidents?
   a. What actions does the IT department 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?
4. What steps would the IT department take to investigate the unusual traffic from HR's payroll servers to an external IP address?

5. What cyber risk assessment(s) has your organization conducted to identify specific threats, vulnerabilities, and critical assets?
   a. What were the outcomes of the assessment(s)?

Module 2

Day 27

Early in the workday, a high volume of employees report that they are unable to log into their <accounts/workstations> using their credentials.

Later that day, a number of <your local government>'s employee workstations display a red screen with a 72-hour timer counting down and the message:

"Every 24 hours there will be a new attack if <your local government> waits to pay the equivalent of $250,000 in Bitcoin. Pay before the time runs out or your system will be wiped."

Due to the ransomware, <Employee pay system/tax revenue system/utility payment system> at <your local government>is no longer functioning.

Day 28

<Your local government> has not paid the ransom. Multiple emergency response organizations (e.g. sheriff offices, emergency dispatch centers, hospitals, etc.) in your jurisdiction are now reporting Distributed Denial of Service (DDoS) attacks. <Insert an emergency response organization from your local government> reports all desktops and Voice over Internet Protocol (VoIP) systems are non-responsive.

Day 29

A social media account from someone claiming to be the attacker contains a warning to <your local government> stating they are serious about the payment deadline. The post starts trending on social media, but skeptical local users comment that the account is fake.

In response, the alleged attacker account begins posting employee personally identifiable information (PII), with captions stating that they have more "for the right price and the longer <your local government> waits to pay, the worse it will get."

Discussion Questions

1. What are your priorities at this point?
2. When would you initiate your incident response plan?
    a. What training have your employees received on the incident response plan?
    b. What actions would you take based on your plan?
    c. Based on the scenario, who are you notifying internally and what is your message?
3. How would your <your local government> mitigate the multiple Distributed Denial of Service (DDoS) attacks?
4. What alternative communications are used if the primary method of Voice over Internet Protocol (VoIP) is inoperable?
    a. How often are these alternative communications tested?
5. When monitoring social media, what types of posts does your organization look for?
    a. What actions would you take if a social media post has misinformation or contains a potential threat?
6. What ransomware policies and procedures are included in your incident response plan?

   a. What is the decision-making process to determine if ransomware will be paid and who makes the final decision?
   b. How are your cyber insurance providers involved in your procedures?
   c. What are the advantages/disadvantages to agreeing/refusing to pay?
   d. What are the potential legal and reputational ramifications?

7. What resources are required for responding to this scenario at this point?
   a. What additional resources do you need to respond to the cyber incident?
   b. What are the processes/procedures to request additional resources?
   c. What mutual aid agreements does <your local government> have with neighboring cities/counties or the state?

Module 3

Day 30

A security researcher contacts your organization concerning <your local government> employee PII being advertised for sale on the dark web.

The emergency response facilities impacted by the DDoS attack are currently relying on <their backup systems/manual operations>.

Day 30 – Afternoon

The deadline for the ransom payment has passed and workstations remain locked. Several employees are reporting to <their payroll office/Human Resources> they have not received direct deposits for the most recent pay period, despite receiving a notification that they have been paid.

Day 31 – 6:00 p.m.

News of the ransomware attack has gone viral on multiple social media platforms with employees and residents using the tag #<your local government>HACKED, stating that your organization does not value their safety.

Discussion Questions

1. How does <your local government> backup its critical systems?
   a. How often are your backups created and/or updated?
   b. How quickly can these backups be deployed?
2. How would <your local government> respond to the news inquiries and the public's comments on social media?
   a. What pre-scripted messages have been developed for cyber incidents?
   b. What training does your communications personnel receive on cyber terminology?
   c. How would public messaging be coordinated and disseminated during a cyber incident impacting the region?
   d. How would <your local government> work to maintain the public's confidence and trust during these incidents?
   e. What are your additional public affairs concerns?
3. When does <your local government> consider a cyber incident to be over/closed?
   a. Who makes this determination?
   b. What post-incident actions or processes would be executed?
4. Based on this scenario, what aspects of <your local government>'s incident response plan needs improvement?

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 local government> 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 local government>'s 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 local government>'s 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 local government> 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 local government>.
    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 local government> 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 local government> 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 local government> utilize multi-factor authentication?
18. Does <your local government>'s 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 local government>, should a vulnerability be identified?
20. What processes does <your local government> 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 local government> retrieve all information technology-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 local government> 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 local government> have? Are they part of the response or continuity planning documents?
27. What is <your local government>'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 local government> 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 <your local government>?
33. Compare and contrast physical and cyber incident notifications and protective action decision-making.
34. 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")?
35. What are the primary and contingency communication mechanisms necessary to support incident management?
36. What multi-factor authentication methods (e.g., something you know, something you have, something you are) does <your local government> utilize to mitigate the potential effects of phishing?
37. If <your local government>'s network is down, what continuity plans and processes would be initiated?
    a. What information would <your local government> report to state partners, if any?
38. What type of cybersecurity clauses do you have in your contract language with entities that have access to your network?
    a. What cybersecurity incidents are your <your local government>'s vendors required to report to you?
39. What type of cybersecurity training are they required to complete before connecting to your networks?

Information Sharing

1. How would <your local government> 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 <your local government> is responsible for addressing those gaps?
    d. What actions, if any, would <your local government> take based on this information?
2. What sources of cybersecurity threat intelligence does <your local government> 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 <your local government>?

3. What mechanisms and products are used to share cyber threat information within your <your local government> and externally (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 local government> 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 local government>?
   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 for taking action and what actions would they take?
   b. How and when would your leadership be notified?
5. How does your <your local government> IT baseline network activity? How would you be able to distinguish between normal and abnormal traffic?
6. How does the <your local government> 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 local government>'s intrusion detection capabilities and analytics that alert you to a cyber incident.
10. What type of hardware and/or software does <your local government> use to detect/prevent malicious activity of unknown origin on your systems/network?
11. What would prompt you or someone in <your local government> 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)?
12. Do you have someone within <your local government> 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 local government> 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 local government> 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 local government>?
        ii. What pre-canned messaging or holding statements does <your local government> have for such an event?
    d. How are you ensuring unity of message between <your local government>, the public, and elected officials?
6. How would these events affect <your local government>'s business operation/processes?
7. What concerns have these incidents generated that have not been addressed?
8. How would <your local government> 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 local government> 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 <your local government>?
        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 local government>'s ability to respond?
    a. What are <your local government>'s established procedures to request additional support?
19. What are <your local government>'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 <your local government> 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 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 local government> 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 primary communications are compromised, how do you provide information to internal and external entities?
26. How would you respond to the attempts to discredit <your local government>'s process on social media?

Recovery

1. When does <your local government> determine a cyber incident is closed?
    a. Who makes this decision?
    b. Would <your local government> engage in any post-incident activities?
2. What actions would <your local government> 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 local government> 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 local government> 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 <your local government> 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 local government>?
   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 local government> 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 <your local government>'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 local government> 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 or county's information systems? How often do they receive the training?
2. How does <your local government> train 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 local government> exercise the plan?
   a. Who is responsible for the exercise planning?
   b. What agencies are involved in the exercise?
   c. What level of the <your local government> 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 local government>'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 local government>?

Senior Leaders and Elected Officials

1. What is your cybersecurity culture? As a leader in your <your local government>, what cybersecurity goals have you set? How have they been communicated?
2. As it relates to <your local government>, what cybersecurity information do you request? What do you receive?
3. What are your cybersecurity risks?
4. Who develops <your local government>'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 risk assessment?
6. What is <your local government>'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 local government> 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 local government> able to do to mitigate it?
13. When did you last receive a cyber threat briefing for <your local government>?
14. How has <your local government> prepared for a cyber incident? Does <your local government> 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 local government> 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 local government>'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 <your local government>'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 local government> 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 local government> respond to the attempts at disinformation/misinformation?
    a. What established public messaging processes does <your local government> have as part of a larger communications plan?
    b. How would <your local government> 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 local government> respond to the emerging news and social media issues?
    a. Does <your local government> 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 local government> have? Does it exercise these policies? If so, how often?
3. What legal documents should <your local government> 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 processes are in place to collect evidence and maintain the chain of custody?

Appendix B: Acronyms

Acronym	Definition
AAR	After-Action Report
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
FBI	Federal Bureau of Investigation
HR	Human Resources
HVAC	Heating, Ventilation, and Air Conditioning
IS	Information Systems
IT	Information Technology
NIST	National Institute of Standards and Technology
PII	Personally Identifiable Information
PPD	Presidential Policy Directive
TLP	Traffic Light Protocol
VoIP	Voice over Internet Protocol

Appendix C: Case Studies

Ransomware Attack Locks 200 County Computers

In October 2020, a state's county experienced a ransomware attack which locked around half of the county's 400 computers. The attackers demanded a $450 ransom to restore each machine, totaling to around $90,000. The compromised computers affected all departments in the county system except the sheriff's office and social services. Included in the attack was the county's Board of Elections systems, which was the priority to restore functionality to, due to the upcoming presidential election. The county refused to pay ransom for any of the computers, and instead opted to restore all computers to their most recent backups. Following the recovery, the county invested $200,000 into upgrading both their hardware and software, including new Windows 365 software for all the county's computers. [1] [2] [3]

Hacktivist Group Claims Responsibility for Attack on City Websites

In June 2020, a U.S. city's websites were taken offline by a hacktivist group who claimed responsibility for the attack. City services experienced disruption due to higher-than-normal traffic on the city's network as the group launched a social media campaign to publicize their efforts. The police department and city's communication channels experienced intermittent outages and were unreliable. The group tweeted throughout the day that "more targets were coming." City services were held at a standstill in response and preparation for further attacks.[4]

Two Dozen Cities Across the Same State Fell Victim to a Coordinated Attack

In August 2019, two dozen cities across a U.S. state fell victim to a coordinated cyber-attack. Municipal computers were held ransom from what is believed to have been a state actor. Multiple systems were affected including police departments, water departments and even library computers. The towns' entire networks had to be shut down. It is believed the hackers gained access to the systems through phishing or a compromised password. One of the affected towns only had a

[1] Evesun. "Chenango County Invests $200,000 in Response to Recent Ransomware Attack." Www.evesun.com, 29 Dec. 2020, www.evesun.com/news/stories/2020-12-29/34092/Chenango-County-invests-. Accessed 9 July 2021.

[2] Eames, Sarah. "Chenango County, N.Y., Computers Hit with Ransomware Attack." GovTech, 28 Oct. 2020, www.govtech.com/security/chenango-county-ny-computers-hit-with-ransomware-attack.html#:~:text=Chenango%20County%2C%20N.Y.%2C%20Computers%20Hit%20with%20Ransomware%20Attack. Accessed 9 July 2021.

[3] Rosenblatt, Josh. "Chenango County Hit with Cyberattack." WBNG, 22 Oct. 2020, wbng.com/2020/10/22/chenango-county-hit-with-cyberattack/. Accessed 9 July 2021.

[4] Gates, B. (2020, June 4). City of Austin websites go down, hackers take credit in protest. *Kxan.com*. https://www.kxan.com/news/local/austin/city-of-austin-websites-down-hackers-anonymous-taking-credit/.

population of 3,600 and it is believed the smaller towns were targeted because of their lower budgets and lack of preparedness.[5]

Ransomware Attack Brings Down County Computers and Servers

In January 2021, the county of a U.S. State suffered a ransomware attack resulting in the encryption of 50 computers and 100 servers. As a result, the county had to isolate the infected devices from the network which brought down some services. It is unknown how much the ransom demand was, but the county refused to pay it, and instead restored their systems using cloud backups. All critical systems were operational within one day of the attack, and remaining systems were restored in the weeks that followed. According to the county, there was minor data loss because not all the servers were properly backed up. Following the attack, the county notified authorities including the FBI. [6] [7]

County School Payroll Accounts Compromised After a Phishing Attack

In 2017, a school of a county in the U.S. was the target of a phishing campaign in their area. As a result, there was a theft of multiple employee payroll accounts and compromised paychecks. This attack amounted to the loss of more than $75,000, and only $3,400 of that amount was recovered. To prevent further risk of future attacks, the district sought assistance with an IT solutions company to implement a phishing monitoring system for emails. [8]

Telephony Denial of Service Attack on a County's Emergency Communications Center

The 911 dispatch center of a U.S. county fell victim to a Telephony Denial of Service (TDoS) Attack in 2016. This was caused by a link that hijacked smartphone users' smartphones when clicked, making it repeatedly dial 911. The communications center was flooded with non-emergency calls at a rate of one approximately every 30 seconds. This mass number of calls preoccupied dispatchers of the center for the 30 minutes the attack lasted but managed to still answer anyone trying to make an emergency call. [9]

[5] DFCBS, W. (2019, August 21). Small Dallas County City of Wilmer Still Operating Despite Ransomware Attack. *CBSDFW.COM*. https://dfw.cbslocal.com/2019/08/21/dallas-county-city-wilmer-operating-ransomware-attack/.

[6] Wilson, David. "California County Focuses on Recovery after Ransomware Attack." GovTech, 19 Feb. 2021, www.govtech.com/security/california-county-focuses-on-recovery-after-ransomware-attack.html. Accessed 9 July 2021.

[7] Rubrik. "Yuba County's Ransomware Remediation Includes Backup and Security." Techwire, 2 June 2021, www.techwire.net/sponsored/yuba-countys-ransomware-remediation-includes-backup-and-security. Accessed 9 July 2021.

[8] McCray, V. "Payday Scam Reported at Fulton County Schools" AJC, 3 October 2017, https://www.ajc.com/news/local-education/payday-scam-reported-fulton-county-schools/SJRK8IMkhfakuNUa9zRHiI/ 3 August 2021

[9] Boone, R. "Lacey Police Arrest Man in Internet Hoax that Flooded Thurston 911 with Non-Emergency Calls" The Olympian, 28 October 2016 https://www.theolympian.com/news/local/article110606177.html, 3 August 2021

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

- https://www.us-cert.gov/ncas/tips/ST04-015
- https://www.us-cert.gov/sites/default/files/publications/DDoS%20Quick%20Guide.pdf
- 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

- https://www.us-cert.gov/ncas/tips/ST04-014
- https://resources.infosecinstitute.com/common-social-engineering-attacks/

Ransomware

Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption, typically in the form of cryptocurrency.

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

- https://www.cisa.gov/stopransomware
- https://www.us-cert.gov/ncas/tips/ST19-001
- https://www.us-cert.gov/ncas/alerts/TA17-132A
- 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

- 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

Key Points of Contact

- Cybersecurity and Infrastructure Security Agency (CISA) (Contact: central@cisa.gov; 888-282-0870)
- 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)

- 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/)
- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; (518) 266-3460)

Other Available Resources

- 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/)
- Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- InfraGard (https://www.infragard.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
- National Council of ISACs (https://www.nationalisacs.org/)

References Cited

"Wannacry Two Years Later: How Did We Get The Data?". (2019, May 27). Retrieved August 22, 2019, from Armis IOT Security: https://info.armis.com/rs/645-PDC-047/images/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: https://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

Evesun. “Chenango County Invests $200,000 in Response to Recent Ransomware Attack.” Www.evesun.com, 29 Dec. 2020, www.evesun.com/news/stories/2020-12-29/34092/Chenango-County-invests-. Accessed 9 July 2021.

Eames, Sarah. “Chenango County, N.Y., Computers Hit with Ransomware Attack.” GovTech, 28 Oct. 2020, www.govtech.com/security/chenango-county-ny-computers-hit-with-ransomware-attack.html#:~:text=Chenango%20County%2C%20N.Y.%2C%20Computers%20Hit%20with%20Ransomware%20Attack. Accessed 9 July 2021.

Rosenblatt, Josh. “Chenango County Hit with Cyberattack.” WBNG, 22 Oct. 2020, wbng.com/2020/10/22/chenango-county-hit-with-cyberattack/. Accessed 9 July 2021.

Gates, B. (2020, June 4). City of Austin websites go down, hackers take credit in protest. Kxan.com //www.kxan.com/news/local/austin/city-of-austin-websites-down-hackers-anonymous-taking-credit/.

DFCBS, W. (2019, August 21). Small Dallas County City of Wilmer Still Operating Despite Ransomware Attack. CBSDFW.COM. https://dfw.cbslocal.com/2019/08/21/dallas-county-city-wilmer-operating-ransomware-attack/.

Wilson, David. “California County Focuses on Recovery after Ransomware Attack.” GovTech, 19 Feb. 2021, www.govtech.com/security/california-county-focuses-on-recovery-after-ransomware-attack.html. Accessed 9 July 2021.

Rubrik. “Yuba County’s Ransomware Remediation Includes Backup and Security.” Techwire, 2 June 2021, www.techwire.net/sponsored/yuba-countys-ransomware-remediation-includes-backup-and-security. Accessed 9 July 2021.

Gates, B. (2020, June 4). City of Austin websites go down, hackers take credit in protest. Kxan.com. https://www.kxan.com/news/local/austin/city-of-austin-websites-down-hackers-anonymous-taking-credit/.

McCray, V. “Payday Scam Reported at Fulton County Schools” AJC, 3 October 2017, https://www.ajc.com/news/local-education/payday-scam-reported-fulton-county-schools/SJRK8IMkhfakuNUa9zRHiI/ 3 August 2021

Boone, R. “Lacey Police Arrest Man in Internet Hoax that Flooded Thurston 911 with Non-Emergency Calls” The Olympian, 28 October 2016 https://www.theolympian.com/news/local/article110606177.html, 3 August 2021