We at PM United believe that knowledge is empowering. We are sharing this CISA sponsored Tabletop Exercise Package for you to use at your own risk. We make no implied or intended endorsement of the content below. If you would like to obtain further information or clarification on the steps herein, please contact our consulting team via email at hello@pmunited.org for a complimentary 30 minute consultation with one of our subject matter experts in Cybersecurity. Enjoy!

PM United LLC

[Enter Organization Name]

CISA Tabletop Exercise Package

Ransomware

<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*": Recipients can spread this to the world, there is no limit on disclosure. This designation is used when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. **Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction.**

This document may be disseminated publicly pursuant to TLP:CLEAR and <exercise sponsor name or other authority> guidelines.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:GREEN

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):GREEN*": Limited disclosure, recipients can spread this within their community. This designation is used when information is useful to increase awareness within their wider community. Recipients may share TLP:GREEN information with peers and partner organizations within their community, but not via publicly accessible channels. TLP:GREEN information may not be shared outside of the community. **Note: When "community" is not defined, assume the cybersecurity/cyber defense community.**

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:GREEN and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):AMBER*": Limited disclosure, recipients can only spread this on a need-to-know basis within their organization and its clients. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organizations involved. Recipients may share TLP:AMBER information with members of their own organization and its clients, but only on a need-to-know basis to protect their organization and its clients and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:AMBER+STRICT

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as *"Traffic Light Protocol (TLP):AMBER+STRICT*: Limited disclosure, recipients can only spread this on a need-to-know basis within their organization. Note that "*TLP:AMBER+STRICT"* restricts sharing to the organization only. This designation is used when information requires support to be effectively acted upon, yet carries risk to privacy, reputation, or operations if shared outside of the organization involved. Recipients may share TLP:AMBER+STRICT information with members of their own organization, but only on a need-to-know basis to protect their organization and prevent further harm.

This document should be disseminated to applicable partners and stakeholders on a need-to-know basis pursuant to TLP:AMBER+STRICT and <exercise sponsor name or other authority> guidelines due to the sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

TLP:RED

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):RED*": For the eyes and ears of individual recipients only, no further disclosure. This designation is used when information cannot be effectively acted upon without significant risk for the privacy, reputation, or operations of the organizations involved. Recipients may therefore not share TLP:RED information with anyone else. In the context of a meeting, for example, TLP:RED information is limited to those present at the meeting.

This document should be disseminated to applicable partners and stakeholders on a strict need-to-know basis pursuant to TLP:RED and <exercise sponsor name or other authority> guidelines due to the extreme sensitivity of the information contained herein.

For questions about this event or recommendations for improvement contact: [Name], [Title] at ###-###-#### or [email address] <of sponsoring organization>.

Exercise Overview

Exercise Name	Exercise Name	
Exercise Date, Time, and Location	Exercise Date Time (e.g. 9:00 a.m. – 12:00 p.m.) Exercise Location	
Exercise Schedule	**Time**	**Activity**
	Time	Activity
	Time	Activity
	Time	Activity
	Time	Activity
	Time	Activity
Scope	X hour, facilitated, discussion-based tabletop exercise	
Purpose	Examine the coordination, collaboration, information sharing, and response capabilities of <Insert Organization> in response to a significant cyber incident.	
INSERT: <NIST, FEMA, or Mission Capabilities>	For example, areas such as Identify, Protect, Respond, etc.	
Objectives	1. Examine the ability for <Insert Organization> to respond to a significant cyber incident. 2. Evaluate the ability for <Insert Organization> to coordinate information sharing during a significant cyber incident. 3. Identify areas of improvement for <Insert Organization>'s cyber incident response plans. 4. Explore processes for requesting additional response resources once internal resources are exhausted. 5. Explore <Insert Organization>'s communications processes for addressing public affairs.	
Threat or Hazard	Cybersecurity Threat	
Scenario	A threat actor targets <Organization>'s system administrator through a phishing email as an entry point into networks/systems. Attackers compromise Personally Identifiable Information (PII), deface public facing websites, and install ransomware on <Organization> computers.	
Sponsor	Exercise Sponsor	
Participating Organizations	Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.).	
Points of Contact	**Insert Organization POC(s)** Contact info	**National Cyber Exercise Program** 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 several events affecting IT users, including an operating system that is no longer supported by its developer, a lost laptop, and a phishing email.
    - **Module 2:** This module includes the discovery of significant data exfiltration possibly including personally identifiable information, unauthorized changes to your website, and ransomware execution.
- 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

It has been one year since the developer of your current operating system announced that they will no longer develop security patches for your operating system. The final security patch was installed last week. This vulnerability was identified in your recently completed annual risk assessment.

Day 2 – 8:00 a.m.

An employee reports to their manager that their work laptop was stolen from their car overnight. The laptop contained sensitive information.

Day 4 – 3:00 p.m.

A Cybersecurity and Infrastructure Security Agency (CISA) Alert is released regarding a new ransomware variant. This ransomware is being used in a campaign targeting state, local, tribal, and territorial governments and private sector firms.

Day 6 – 10:00 a.m.

A system administrator from the Information Technology (IT) Department receives an email from the personal email account of a human resources (HR) employee. The system administrator and HR employee are connected via professional networking websites. The email notes that the HR employee recently noticed some discrepancies in their 401K withholdings and recommends that the system administrator review their own account information. The system administrator clicks on the link in the email and is re-directed to what appears to be the legitimate 401K website. The IT employee does not believe the email to be suspicious.

Discussion Questions

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

1. What are the greatest cyber threats to your organization?
2. What cybersecurity threat intelligence does your organization receive?
    a. What cyber threat information is most useful?
    b. Who is responsible for collating information across your organization?
    c. What actions would your organization take following an alert like the one presented in the scenario?
3. What patch management plans does your IT department utilize?
    a. What procedures are followed to evaluate each server's criticality and applicability to software patches?
4. 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?
5. 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?

6. 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)?
7. What considerations are addressed in your risk management strategy? (e.g., extended downtime, impaired functionality, loss of data, etc.)

Module 2

Day 7 – 12:30 p.m.

IT conducts their routine review of intrusion detection system logs and discovers unusual traffic on your organization's printer ports. There is a significant amount of data leaving the printer ports and going to external IP addresses.

Day 8 – 3:30 p.m.

Employees notice several cosmetic changes to the organization's website and report to IT. They also note that a commonly used link now directs users to an unrelated website.

Day 9 – 9:00 a.m.

Computers throughout your organization now display a blank red screen. A ransom message then appears demanding <Insert Ransom Amount (e.g., $53,000.00)> worth of bitcoin for the decryption key and a warning that the key will expire unless payment is received within 48 hours.

Day 10 – 9:30 a.m.

A security researcher uncovers a series of posts from a well-known hacker group on the Dark Web and contacts your organization. The researcher believes that the posts are genuine and the threat actors have gained access to personally identifiable information (PII), including <employee social security numbers, bank account and routing number information, etc.>. The hacker group has provided a small number of data records to verify their claims and are willing to sell the information for "the right price."

Day 11 – 10:00 a.m.

Overnight the tag #<Insert Organization>HACKED goes viral on multiple social media platforms. Several news media outlets contact your organization seeking comment about your ransomware infection and the data breach.

Discussion Questions

1. What are your organization's priorities at this point?
2. How does your organization baseline network activity?
    a. How would you be able to distinguish between normal and abnormal traffic?
3. How would these incidents be assessed according to your organization's cybersecurity incident severity levels and/or escalation criteria?
4. What actions would be taken according to your organization's cyber incident response plan?
    a. What training have your employees received on this plan?
    b. What actions would you take based on the plan?
5. What internal and external notifications would your organization need to make?
    a. What would be your internal and/or external message?
6. What is your organizations decision-making process for ransomware payment?
    a. What ransomware policies and procedures are included in your incident response plan?
    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 impact will the sale of sensitive or PII have on your response and recovery activities?
    a. What additional legal and/or regulatory notifications could this incident possibly trigger?

8. What capabilities and resources are required for responding to this scenario?
    a. What additional resources would you need to respond to the cyber incident?
    b. What are the processes/procedures to request additional resources?
9. How would your organization respond to the news media reports?
    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?
    d. How would your organization work to maintain the public's confidence and trust during these incidents?
    e. What staff does your organization have to monitor and manage your social media presence?
    f. What are your additional public affairs concerns?

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.*

Identify

1. What are your most significant threats and vulnerabilities?
    a. What cyber risk assessment(s) has/have your organization conducted to identify organization-specific threats and vulnerabilities?
    b. What are your highest cyber security risks?
    c. What are your concerns with the threats and vulnerabilities surrounding your organization?
2. How does your organization integrate cybersecurity into the system development life cycle (i.e., design, procurement, installation, operation, and disposal)?
3. Discuss the role of cybersecurity in relation to third-party support vendors and crucial suppliers.
    a. What types of concerns and risks do you discuss with them?
4. Discuss your supply chain concerns related to cybersecurity.
5. What role does organizational leadership play in cybersecurity?
    a. How does this role differ during steady-state and incident response?
6. What level of funding and/or resources are devoted to cyber preparedness?
    a. Based on your risk assessment, what is the range of potential losses from a cyber incident?
    b. How have you assessed if current funding is enough to cover the greatest potential loss from a cyber incident?
7. Discuss cyber preparedness integration with your current all-hazards preparedness efforts.
    a. Who are your cyber preparedness stakeholders (public, private, non-profit, other)?
8. What mission essential functions depend on information technology and what are the cascading effects of their disruption?
9. What external reviews or audits of your IT plans, policies, or procedures have been conducted within the last year?
    a. How often do you have your employees review IT plans, policies, and procedures?
    b. What cybersecurity awareness training is provided for employees?
10. Discuss the current network security architecture for crucial suppliers with remote access.
11. What background checks are conducted for IT, security, and key supporting personnel?
12. Who is in charge of cybersecurity management for your organization?
    a. What additional support do they have within the organization?
13. How does your organization recruit, develop, and retain cybersecurity staff?
    a. What credentials are important for your cybersecurity staff to have/obtain?
14. What cyber threat information does your organization receive?
    a. Through what channels would this information be received and disseminated?
    b. What established mechanisms are in place to facilitate rapid information dissemination?
    c. What are your organization's known communication gaps?

   d. What actions would your organization take based on the information presented in the scenario?
15. What other sources of cybersecurity threat intelligence does your organization receive? For example, information from Federal Bureau of Investigation (FBI), InfraGard, open source reporting, security service providers, others?
    a. What cyber threat information is most useful to your organization?
    b. Is the information you receive timely and actionable?
    c. Who is responsible for collating information across the organization?
16. 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)?
17. Describe how variables in threat information (timeframe, credibility, and specificity) impact decision making.
18. 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?

Protect

1. What established cybersecurity governance (laws, regulations, and/or government policies) does your organization follow?
2. How is cybersecurity integrated into both organizational and project risk assessments and management?
3. How does your organization respond to personnel failings to comply with established information security policies and procedures?
4. When was the last time your organization's cybersecurity incident response plan was reviewed?
    a. When was the plan last tested?
    b. How often is the plan revised?
    c. Which departments or agencies are required to follow the plan?
5. Where and how does your organization utilize multi-factor authentication to mitigate the potential effects of phishing?
6. What active measure(s) does your organization employ to prevent distributed denial of service (DDoS) attacks against your websites and operational systems?
7. How does your organization track and/or identify problematic pieces of firmware in your organization, should a vulnerability be identified?
8. 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. When 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?
    c. Where are the procedures for these actions documented?
9. What third-party vendors have access to your network?
    a. How much access do third-party vendors have to your network?

   b. What protections do you have in place to protect against malicious intent by those vendors or outside parties that have access to your network?
10. Discuss the status of cyber preparedness planning within your organization.
   a. What were the results of your organization's business impact analysis (BIA)?
   b. What information technology (IT) infrastructure supporting mission essential functions were identified in the BIA continuity of operations and continuity of government plans?
   c. How is cybersecurity integrated in your business continuity plans?
   d. How does your business continuity and/or disaster recovery planning prioritize different parts of your information technology infrastructure for restoration?
   e. How have IT specific plans been coordinated with other planning efforts such as an Emergency Operations Plan or Continuity of Operations Plan?
11. According to your organization's policies, plans, and procedures, as well as government guidance and regulations, what are your identified responsibilities for preventing cyber incidents?
   a. What are your organization's capabilities to prevent cyber incidents?
12. Who is responsible for network and information security management?
13. Does your Emergency Operations Plan have a Cyber Incident Annex?
   a. When was the annex last revised?
   b. Who is responsible for maintaining the annex?
   c. How closely does the annex align with your Cyber Incident Response Plan?
14. Can you identify key documents that support cyber preparedness at a federal, state, or local level? (Presidential Policy Directive (PPD) 41: United States Cyber Incident Coordination, National Cyber Incident Response Plan (NCIRP), PPD 21: Critical Infrastructure Security and Resilience, Executive Order: Improving Critical Infrastructure Cybersecurity, National Response Framework (NRF), National Infrastructure Protection Plan (NIPP), National Institute of Standards and Technology (NIST) Cybersecurity Framework, etc.)
15. Which cybersecurity standards of practice (NIST Cybersecurity Framework/800 Series, ISO/IEC, etc.) does your organization follow?
   a. How are these standards integrated into your cybersecurity policies?
16. What flowcharts does your organization have to show the high-level relationships and crisis lines of communication (i.e., who calls who) specifically for a cyber incident?
17. How does your organization handle IT account management?
   a. What formal or informal policies and procedures does your organization have related to IT account management?
   b. What protocols for establishing, activating, modifying, disabling, and removing accounts are included in these policies or procedures?
   c. What protocols/steps for notifying IT account managers/administrators when users are terminated are included in these policies and procedures?
18. Describe the current relationships between IT, business continuity functions, and physical security.
   a. How are their efforts coordinated?
   b. How do they collaborate with public relations, human resources, and legal departments?
19. What processes ensure that your external dependencies (contractors, power, water, etc.) are integrated into your security and continuity planning and programs?
20. Describe the decision-making process for protective actions in a cyber incident.
   a. What available options have been documented in plans?

   b. How are they activated?
21. What immediate protection and mitigation actions would be taken at your organization in this scenario?
   a. Who is responsible for those actions, and are they fully aware of those responsibilities?
22. What protective actions would you take across non-impacted systems or agencies in the scenario presented?
   a. How are actions coordinated across parts of the organization?
   b. Who is responsible for protective action decision-making, and are they fully aware of those responsibilities?
23. What gaps can you identify in your current physical and cyber incident notifications and protective action decision-making processes?

Detect

1. How do employees report suspected phishing attempts?
   a. What actions does your department take when suspicious emails are reported?
   b. What are the formal policies or plans that would be followed?
   c. How often does your department conduct phishing self-assessments?
2. What processes are in place for employees to report suspected cyber incidents?
   a. How are employees trained on this process?
3. What is your cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
   a. What actions would be taken at this point?
   b. When is leadership be notified?
   c. When are external organizations notified?
4. How would you be able to distinguish between normal and abnormal traffic?
   a. How does your organization baseline network activity?
5. Who do you report cybersecurity incidents to outside your organization?
   a. What mandatory reporting requirements do you have?
6. When would your organization begin to suspect the HVAC/Fire alarm issues might be the result of malicious cybersecurity activity?
7. Who would you inform internally if you receive the email demanding bitcoin payment?
   a. Who would you inform externally?
8. What detection and analysis procedures does your organization have for loss of personally identifiable information (PII)?
   a. How do detection and analysis procedures differ for loss of PII, phishing attempts, data exfiltration, data modification, or other incidents?
9. According to your organization's severity schema, what level would you classify this incident?
   a. What additional notifications or actions would this prompt?
10. Who is responsible for correlating information when an incident spans different organizational levels?
11. What internal resources and capabilities are available to analyze the intrusions?
   a. What external resources are available from government partners?
   b. What external resources exist are available within the private sector?
12. How is information shared among your internal and external stakeholders?
   a. What formal information sharing policies and procedures does your organization utilize?

   b. What information sharing mechanisms are used by your organization?
13. What intrusion detection capabilities does your organization have?
   a. How do they alert you to a cyber incident?
14. What type of hardware and/or software does your organization use to detect/prevent malicious activity of unknown origin on your systems/network?

Respond

1. What is your planned cyber incident management structure?
   a. Who leads incident management in each department?
   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")?
   e. What are the primary and contingency communication mechanisms necessary to support incident management?
2. Who within your organization monitors the Dark Web?
   a. How would they verify the security researcher's claims and confirm authenticity of the sensitive information in question?
3. 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?
4. 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?
5. What response actions would your organization have taken at this point? Are these actions driven by a plan?
6. What impact will the sale of sensitive or Personally Identifiable Information (PII) have on your response and recovery activities?
   a. What authorities would need to be notified?
   b. Have your public relations priorities changed?
   c. What legal or regulatory notifications would be triggered?
7. What internal and external notifications would be required for this scenario?
   a. What process or plan outlines the severity thresholds for which notifications are made and what information is to be conveyed?
   b. How is senior leadership being updated and what information is provided?
   c. How are you coordinating public messaging within your organization?
   d. What pre-canned messaging or holding statements could be used for such an event?
8. How are you ensuring unity of message between your organization, the public sector, and elected officials?
9. How would these events affect your organization's business operation/processes?
10. Which of these issues would be considered a cyber incident at this point?
11. What additional concerns do these incidents generate?
12. How would your organization respond to the discovery of a malicious, unauthorized administrator account on your systems?
   a. Who would be informed internally?

   b. Who would be informed externally (e.g. law enforcement, cybersecurity insurance partners, etc.)?
13. What resources are required for incident investigation and attribution?
   a. How sufficient would your internal resources be based on this scenario?
14. What events presented in the scenario would trigger activation of your emergency operations plan cyber incident annex?
   a. At what point in the scenario would you contact law enforcement and/or the state Attorney General?
   b. How would relationships with law enforcement and other partners be managed?
   c. How does a law enforcement investigation impact containment, eradication, and recovery efforts?
15. What processes and resources are in place for evidence preservation and collection?
16. Discuss the difference between network and host forensics.
   a. How are you equipped and staffed to address this?
17. What are the roles of a network and/or security operations center during a response?
18. What are your essential elements of information and key information questions necessary for operational and executive-level responses to cyber incidents?
19. What mission essential functions are impacted by the incidents described in the scenario?
20. How does your organization maintain service availability of key assets (e.g., network connectivity, etc.)?
   a. What capabilities and resources are required for responding to this series of incidents?
   b. What internal resources do you depend on and are they sufficient?
   c. Whom do you contact if you're in need of additional third-party assistance?
   d. What resources are available within the state or locally and how do you request them?
   e. 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?
21. What are the procedures to request additional support for incident response once your organization's ability is exhausted?
22. What are your organization's response priorities?
   a. Who would be notified at this point in the scenario?
   b. What response actions would the IT/IS department take at this point?
   c. What response capabilities and resources are required to respond to these incidents?
23. What documented actions would be required when the exfiltration is discovered?
24. What is your organizations decision-making process for ransomware payment?
   a. What ransomware policies and procedures are included in your incident response plan?
   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?
   e. What are the political ramifications?

   f. What outside partners/entities do you need to contact?

25. Where do you receive cyber response technical assistance?
    a. What are the plans, procedures or policies in place to access this assistance?
26. How has your organization identified and established relationships with your service provider for incident/breach response issues (e.g., credit counseling, forensic/computer security services)?
    a. What are some challenges that are experienced by information technology and business continuity planning in terms of information sharing?
27. 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?

Recover

1. When does your organization determine a cyber incident is closed?
   a. Who makes this decision?
   b. In what post-incident activities would your organization engage?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
   a. What are the risks associated with re-activating critical business processes and systems?
   b. When would your organization consider a complete rebuild of these systems?
   c. How long and costly would a complete rebuild of systems be?
   d. 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. What back-ups of vital records does your organization have in a location that is separated from your primary working copies of your files?
   a. How long do you keep any copies of archived files backed up?
   b. 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?
6. Describe your role in post-incident activity.
7. How would you work with critical infrastructure providers to determine the incident is over?
8. How does post incident-activity differ when critical infrastructure is involved?
9. Describe your organization's continuity of operations plan (COOP) for functions at a location separate from your main building
   a. How would a suspected cyber incursion impact your organization's ability to activate its COOP Plan?
10. What alternative systems or manual processes are in place to continue operations if a critical system is unavailable for a significant period of time?
    a. Who can authorize the use of alternate systems or procedures?

Training and Exercises

1. What cybersecurity and/or IT security awareness training does your organization provide to all users?
   a. What is covered in your training (e.g. password procedures, prominent cyber threats, how to report suspicious activities, etc.)?

   b. How often is training provided?
   c. What training is provided to managers and executive leaders?
   d. Is training required to obtain network access?
   e. What security-related training does your department or agency provide to, or require of, IT personnel and vendors with access to your systems/network?
2. What special training does your cybersecurity incident response team members undergo to detect, analyze, and report this activity?
   a. How well is your staff trained to read and analyze your intrusion detection system logs?
3. What training do you provide in support of your Cybersecurity Incident Response Plan, Business Continuity Plan, Emergency Operations Plan Cyber Incident Annex, or other related plans?
4. How often does your organization exercise your cyber incident response 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?
5. How do your organization's annual Training and Exercise Planning Workshop and Multi-Year Training and Exercise Plan address cybersecurity?
6. What are your cybersecurity incident response team's exercise requirements?
7. How does your organization's exercise efforts include both physical and cyber risks?
   a. How do senior or elected officials participate in your exercises?
8. What additional training and/or exercising is required by your organization?

Senior Leaders and Elected Officials

1. What is your organization's cybersecurity culture?
   a. As a leader in your organization, what cybersecurity goals have you set?
   b. How have these goals been communicated?
2. What cybersecurity information do you request relating to your jurisdiction?
   a. What information do you receive?
3. What are your primary cybersecurity risks?
4. Who develops your jurisdiction's cybersecurity risk profile?
   a. What are the reporting requirements (e.g., Directed to, required by statute, or other)?
   b. How often do they report?
5. How is cybersecurity integrated with physical risk for an integrated jurisdictional risk assessment?
6. What is your jurisdiction's greatest cybersecurity concern?
   a. Why do you rate this concern as your greatest concern?
   b. Who reports to you on cyber threats?
7. What 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?
12. What is the greatest threat facing your critical infrastructure?
    a. What is your jurisdiction able to do to mitigate it?
13. What cyber threat briefings have you received for your jurisdiction?

14. How has your jurisdiction prepared for a cyber incident?
    a. What cybersecurity plans does your jurisdiction have formalized?
    b. How does the plan outline the collaboration of your information security officers?
15. How have your information security officers and emergency managers jointly planned for cybersecurity incidents?
16. What are your cybersecurity workforce gaps?
    a. 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 your notification?
    a. What is the documented notification process?
19. What requirements or agreements exist for critical infrastructure to notify you of a cyber incident?
20. 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?
    a. What parts of the government need to be engaged (e.g. state, local, federal)?
23. When would your jurisdiction's Emergency Operations Center be activated in a cyber incident?
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?

Media

1. What are your public affairs concerns?
    a. Who is responsible for coordinating the public message?
    b. How would your department respond to the local media reports?
    c. What information are you sharing with citizens? Employees?
    d. What training on cyber terminology is conducted for public information personnel to manage cyber incident related messaging?
    e. What pre-drafted statements could your department use to respond to media outlets?
    f. How does your organization manage its social media presence?
    g. What guidance is provided to employees regarding interaction with public media outlets during incidents?
2. What information would your organization communicate to the public?
3. Who is responsible for public information related to the incident? What training or preparation have they received?

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 is included your state's security breach notification laws?

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

Appendix C: Case Studies

Malware Infection

On an early morning in February 2022, a satellite telecommunications provider experienced the start of a multifaceted cyberattack.[1] The incident began with a targeted distributed denial of service (DDoS) attack coming from company-provided consumer equipment. Later, tens of thousands of their modems went offline and did not reconnect to the service provider. It was later discovered that the cause of this was a malicious program nicknamed "AcidRain." This malware was designed to systematically delete essential files on UNIX operating systems, such as the ones used by this provider's modems. Once critical data was erased, the malware would reset the devices making the modems unusable until restored to factory settings.

A forensic investigation by the telecommunications provider revealed that the malware was activated with "a legitimate management command" sent by a malicious actor with unauthorized access to their internal network. Thousands of customers had temporarily lost connection to the internet over the course of this cyberattack. The provider began shipping almost 30,000 functional modems out to the affected customers following the attack, likely inflicting additional financial costs.

Distributed Denial of Service Attack

In September 2021, several Voice over Internet Protocol (VoIP) service providers around the world experienced massive disruptions in service due to a series of DDoS attacks.[2] These attacks continued for over a week, making it difficult for customers to hold online calls. One service provider even reported they were having trouble to providing Enhanced 911 services and web portal access to their clients.[3]

Additionally, the attack had major financial consequences for the impacted providers. The threat actors requested a $4.5 million ransom, though payment decisions from the providers has not been disclosed. However, one service provider reported that the attack had cost them "between $9 million and $12 million" in revenue.[4]

Social Engineering – Phishing

In July 2021, a university healthcare organization disclosed that it had experienced a data breach caused by a phishing attack. Threat actors were able to obtain valid credentials though malicious

---

[1] Viasat Corporate. (2022, March 30). *KA-SAT Network cyber attack overview*. Viasat. https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

[2] Mayank Sharma. (2021, September 28). *DDoS assaults against VoIP providers continue.* Techradar. https://www.techradar.com/news/ddos-assaults-against-voip-providers-continues

[3] Lawrence Abrams. (2021, September 27). *Bandwidth.com is latest victim of DDoS attacks against VoIP providers*. Bleeping Computer. https://www.bleepingcomputer.com/news/security/bandwidthcom-is-latest-victim-of-ddos-attacks-against-voip-providers/

[4] U.S. Securities and Exchange Commission. (2021, October 26). *Bandwidth Announces Preliminary Third Quarter 2021 Revenue Results Exceeding Guidance and Estimated Full Year Revenue Impact of DDoS Attack*. https://www.sec.gov/Archives/edgar/data/1514416/000151441621000280/q32021exh991-preliminaryth.htm

emails they sent to employees.[5] Using the gathered stolen credentials, the threat actors gained unauthorized access to the organization's emails from December 2020 to April 2021. The organization reported that the personally identifiable information (PII) and protected health information (PHI) of nearly 500,000 employees, patients, and students may have been compromised. [6] This information would include names, social security numbers, and medical images and diagnoses. The incident was reported to the Federal Bureau of Investigation (FBI), and the organization has since enhanced its security controls.

Ransomware

In January 2022, a large county in the United States experienced a ransomware attack that took office computers and several department websites offline. This caused county offices to close for several days, while the sheriff's department and Emergency Medical Services (EMS) operated on their backup contingencies.[7] The local detention center lost access to its automated door and camera systems because of this ransomware attack. Additionally, $191,000 worth of employee laptops were reported as damaged.[8]

County representatives stated they did not pay the ransom demands and used their cyber insurance coverage to aid in recovery processes.[9] The County's Chief Information Officer (CIO) later said multifactor authentication (MFA) would be implemented for all users to enhance security controls. Additionally, the county commission also accepted a new cybersecurity policy following the incident.

---

[5] Gatlan, S. (2021, July 27). *UC San Diego Health discloses data breach after phishing attack*. BleepingComputer. https://www.bleepingcomputer.com/news/security/uc-san-diego-health-discloses-data-breach-after-phishing-attack/

[6] Freeman, M. (2021, September 24). *UC San Diego Health sued over data breach that may have exposed records of 500,000 patients*. San Diego Union-Tribune. https://www.sandiegouniontribune.com/business/story/2021-09-23/sd-fi-ucsandiego-cyber-attack#:%7E:text=UC%20San%20Diego%20Health%20faces%20a%20lawsuit%20over,and%20others%20connected%20with%20the%20health%20care%20system.

[7] Associated Press. (2022, January 5). *Bernalillo county reports suspected ransomware attack*. U.S. News & World Report. https://www.usnews.com/news/best-states/new-mexico/articles/2022-01-05/bernalillo-county-reports-suspected-ransomware-attack

[8] Salcedo, A. (2022, January 26). *Bernalillo county moving forward after ransomware attack*. KOAT. https://www.koat.com/article/bernalillo-county-recovers-ransomware-attack/38892305

[9] Dyer, J. (2022, April 28). *Bernalillo county issues an upgrade to cybersecurity policy after hack*. Albuquerque Journal. https://www.abqjournal.com/2493604/bernco-strengthens-cybersecurity-policies.html

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 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

- CISA Ransomware (https://www.cisa.gov/stopransomware)
- 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

- 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.dhs.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 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/)
- 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/)
- 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

Viasat Corporate. (2022, March 30). KA-SAT Network cyber attack overview. Viasat. https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/

Mayank Sharma. (2021, September 28). DDoS assaults against VoIP providers continue. Techradar. https://www.techradar.com/news/ddos-assaults-against-voip-providers-continues

Lawrence Abrams. (2021, September 27). Bandwidth.com is latest victim of DDoS attacks against VoIP providers. Bleeping Computer. https://www.bleepingcomputer.com/news/security/bandwidthcom-is-latest-victim-of-ddos-attacks-against-voip-providers/

U.S. Securities and Exchange Commission. (2021, October 26). Bandwidth Announces Preliminary Third Quarter 2021 Revenue Results Exceeding Guidance and Estimated Full Year Revenue Impact of DDoS Attack. https://www.sec.gov/Archives/edgar/data/1514416/000151441621000280/q32021exh991-preliminaryth.htm

Gatlan, S. (2021, July 27). UC San Diego Health discloses data breach after phishing attack. BleepingComputer. https://www.bleepingcomputer.com/news/security/uc-san-diego-health-discloses-data-breach-after-phishing-attack/

Freeman, M. (2021, September 24). UC San Diego Health sued over data breach that may have exposed records of 500,000 patients. San Diego Union-Tribune. https://www.sandiegouniontribune.com/business/story/2021-09-23/sd-fi-ucsandiego-cyber-attack#:%7E:text=UC%20San%20Diego%20Health%20faces%20a%20lawsuit%20over,and%20others%20connected%20with%20the%20health%20care%20system.

Salcedo, A. (2022, January 26). Bernalillo county moving forward after ransomware attack. KOAT. https://www.koat.com/article/bernalillo-county-recovers-ransomware-attack/38892305

Dyer, J. (2022, April 28). Bernalillo county issues an upgrade to cybersecurity policy after hack. Albuquerque Journal. https://www.abqjournal.com/2493604/bernco-strengthens-cybersecurity-policies.html