[Enter Organization Name]

CISA Tabletop Exercise Package – Insider Threat

<Exercise Date>

U.S. Department of Homeland Security
Cybersecurity and Infrastructure Security Agency

<Exercise Title>
Situation Manual

Table of Contents

Handling Instructions

Delete instructions that are not applicable.

TLP: AMBER [Delete this qualifier]

The title of this document is <Exercise Title> Situation Manual. This document is unclassified <if applicable> and designated as "*Traffic Light Protocol (TLP):AMBER*"<if applicable> 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: GREEN [Delete this qualifier]

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: RED [Delete this qualifier]

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>.

TLP: WHITE [Delete this qualifier]

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>.

Exercise Overview

Exercise Name	Exercise Title	
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
	Time	Activity
	Time	Activity
	Time	Activity
Scope	X hour facilitated, discussion-based Tabletop Exercise	
Purpose	To evaluate the effectiveness of <Organization> plans for managing a response to an insider based cyber threat.	
INSERT: <NIST, FEMA, or Mission Capabilities>	For example, areas such as Identify, Protect, Respond, etc.	
Objectives	1. Evaluate <Organization's> ability to track and respond to supply chain-oriented threats. 2. Explore potential vulnerabilities that may exist in <Organization's> relationship with its third-party vendors. 3. Evaluate <Organization's> ability to restore operations from back-up files.	
Threat or Hazard	Cyber	
Scenario	A disgruntled former employee takes advantage of his new position at one of your third-party vendors to exploit vulnerabilities in your systems created by a supply chain issue.	
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	DHS CISA Exercises CEP@hq.dhs.gov CISAServiceDesk@us-cert.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.
Evaluators 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 a microprocessor vulnerability requiring an expensive replacement process and a disgruntled employee who threatens the organization.
    - **Module 2:** This module presents an unknown attacker exploiting the vulnerability identified in Module 1 and the loss of critical files and data.
- Hotwash

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: 9:30 a.m.

A Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) Alert is released regarding a vulnerability with a type of microprocessor that is widely deployed in your organization. This vulnerability may allow an attacker access to sensitive data.

Day 8: 4:45 p.m.

After investigating the vulnerability, your Information Technology (IT) department determines it will be necessary to replace the impacted piece of hardware. As the replacement process will be expensive and labor intensive, it is determined that a year-long roll out and update strategy should be implemented. The IT department will develop the replacement process in coordination with representatives from all major departments in your organization.

Day 10: 12:30 p.m.

During a lunch meeting regarding the roll out process, one of the representatives of a key department loudly berates team members from other departments using language that falls far outside your <Organization's> definition of acceptable. This representative, while highly competent in his field, has engaged in similar behavior in the past and had been formally cautioned by Human Resources that additional behavior of this nature will result in termination.

Day 10: 2:30 p.m.

Senior management makes the decision to terminate the employee for his abusive behavior. He reacts badly to the notification, screaming expletives at senior management, and telling them that "They will be sorry!" for firing him.

Discussion Questions

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

1. Would your organization receive the Alert described in the scenario?
    a. Through what channels would this information be received and disseminated?
    b. Are there established mechanisms to facilitate rapid information dissemination?
    c. What actions, if any, would your organization take based on this information?
2. What sources of cybersecurity threat intelligence does your organization receive? For example, information from CISA, Federal Bureau of Investigation (FBI), open source reporting, security service providers, others?
    a. What cyber threat information is most useful?
    b. Is the information you receive timely and actionable?
    c. Who is responsible for collating information across the organization?
3. Do you have a method for tracking and/or identifying problematic firmware in your organization, should a vulnerability be identified?
4. What processes does your organization have in place for when an employee is terminated or resigns?
    a. Are there any additional processes that are implemented if the employee's termination is contentious?

b. 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?

Module 2:

Day 13: 9:00 a.m.

Staff begin the process of replacing impacted chips, but due to high demand for replacement materials, they estimate the process will not be fully completed for 18 months.

Day 23: 3:30 p.m.

During a meeting with one of your key third-party vendors, it is revealed that they have hired the employee that your organization terminated for abusive behavior. The vendor assures your representatives that the employee will not be present at any meetings with your organization.

Day 42: 4:00 p.m.

Several employees contact the help desk with complaints of difficulties accessing information on shared network drives. Some files appear to have been renamed, moved, or deleted. The IT department can recover the missing files from back-ups, but any work that had been completed following the creation of the latest back-up has been lost.

Day 43: 9:30 a.m.

The IT department reviews logs to determine the issue with the files. They quickly identify the presence of an administrator-level account that should not be on the system. The account is immediately deactivated.

Day 44: 4:00 p.m.

The IT department determines the unknown administrator account was added to the system by exploiting the microprocessor vulnerability on a machine that was deemed to be a low priority for replacement. After accessing the memory of the machine, the attacker was able to obtain an administrator password that had been used to install a recent security patch, create a new administrator account, and move laterally through the system.

Day 46: 10:00 a.m.

The IT department determines that the Internet Protocol address used to create the unauthorized administrative account belongs to your third-party vendor.

Day 46: 12:00 p.m.

Staff are frantically calling your support desk. Files crucial to your organization's ability to complete its core functions appear to have been deleted.

Discussion Questions

1. Does your organization have back-ups of vital records/files in a location that is separated from the primary records/files?
    a. How long do you keep back-up files?
    b. How long will it take to restore files from your back-ups?
2. How would your organization respond to the discovery of an unauthorized administrator account on your systems?
    a. Who would you notify?
    b. Would you make any external notifications? (e.g. law enforcement, cybersecurity insurance partners, etc.)?
3. What protection and mitigation actions would you take based on the events in this scenario?

   a. Who is responsible for those actions?
4. What resources are required for incident investigation and response?
   a. Are sufficient resources available internally?
5. Do any third-party vendors have access into your network?
   a. What protections do you have in place to protect against malicious intent by those vendors or outside parties that have access to your network?
6. Are alternative systems or manual processes in place to continue operations if a critical system is unavailable for a significant amount of time?
   a. Who can authorize use of alternate systems or procedures?
7. What is your top priority: mitigation of the incident (resolving the issue) or investigation (preserving the evidence to build a criminal case)?
   a. Who would make this decision?
   b. Are mitigation and investigation mutually exclusive?
8. At what point in the scenario would you contact law enforcement?
   a. How would relationships with law enforcement and other partners be managed? Where is the process documented?
   b. Does a law enforcement investigation impact containment, eradication, and recovery efforts?
   c. Are processes and resources in place for evidence preservation and collection?

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. Has your organization conducted a cyber risk assessment to identify organization-specific threats and vulnerabilities?
    a. What are your most significant threats and vulnerabilities?
    b. What are your highest cyber security risks?
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 contracts with third-party support vendors and crucial suppliers. Have you discussed these types of concerns and risks with them?
4. Discuss your supply chain concerns related to cybersecurity.
5. What role does organizational leadership play in cybersecurity? Does this role differ during steady-state and incident response?
6. 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?
7. Discuss cyber preparedness integration with your current all-hazards preparedness efforts. 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. Have you had any external review or audit of your IT plans, policies, or procedures within the last year?
10. Discuss the current network security architecture for crucial suppliers with remote access.
11. Are background checks conducted for IT, security and key supporting personnel?
12. Is there a manager/department in charge of cybersecurity management? If yes, is this the primary function of that manager?
13. How does your organization recruit, develop, and retain cybersecurity staff?
14. Would your organization receive the information presented in the scenario?
    a. Through what channels would this information be received and disseminated?
    b. Are there established mechanisms to facilitate rapid information dissemination?
    c. Are there known communication gaps? If so, who in your organization is responsible for addressing those gaps?
    d. What actions, if any, would your organization take based on this information?
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?
    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. Does your organization have established cybersecurity governance? When was it signed?
2. How is cybersecurity integrated into both organizational and project risk assessments and management?
3. Does your organization employ a formal sanctions process for personnel failing to comply with established information security policies and procedures? If so, has this been communicated to employees?
4. Does your organization have a cybersecurity incident response plan? When was it issued? When was the incident response plan last revised? What authorities require which departments or agencies to follow the plan?
5. Does your organization utilize multi-factor authentication to mitigate the potential effects of phishing?
6. Does your IT department have a patch management plan in place? If so,
    a. Are risk assessments performed on all servers on the network?
    b. Are processes in place to proactively evaluate each server's criticality and applicability to software patches?
    c. Does this plan include a risk management strategy that addresses the following considerations?
        i. The risks of not patching reported vulnerabilities?
        ii. Extended downtime?
        iii. Impaired functionality?
        iv. The loss of data?
7. What active measure(s) does your organization employ to prevent denial of service (DDoS) attacks against your websites and operational systems?
8. Do you have a method for tracking and/or identifying problematic pieces of firmware in your organization, should a vulnerability be identified?
9. What processes does your organization have in place for when an employee is terminated or resigns?
    a. Are there any additional processes that are implemented if the employee's termination is contentious?
    b. 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?

10. Do any third-party vendors have unmitigated access into your network?
    a. What protections do you have in place to protect against malicious intent by those vendors or outside parties that have access to your network?
11. Discuss the status of cyber preparedness planning within your organization.
    a. Have you completed a business impact analysis? Does the analysis include information technology (IT) infrastructure supporting mission essential functions identified in continuity of operations and continuity of government plans?
    b. 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?
12. What are your identified responsibilities for, and capabilities to, prevent cyber incidents?
13. Who is responsible for network and information security management?
14. Does your Emergency Operations Plan have a Cyber Incident Annex? When was it last revised? Who is responsible for maintaining the annex?
15. 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.)
16. Does your organization follow a cybersecurity standard of practice (NIST Cybersecurity Framework/800 Series, ISO/IEC, etc.)? If so, which?
17. Are there flowcharts showing the high-level relationships and crisis lines of communication (i.e., who calls who) specifically for a cyber incident? Are they part of the response or continuity planning documents?
18. Does your organization have a 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?
19. Are IT and business continuity functions coordinated with physical security? Are all three then collaborating with public relations, human resources, and legal departments?
20. Do you have processes to ensure that your external dependencies (contractors, power, water, etc.) are integrated into your security and continuity planning and programs?
21. 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?
22. What immediate protection and mitigation actions would be taken at your organization in this scenario? Who is responsible for those actions?
23. What protective actions would you take across non-impacted systems or agencies in the scenario presented? Who is responsible for protective action decision-making? How are actions coordinated across parts of the organization?

24. Compare and contrast physical and cyber incident notifications and protective action decision-making.

Detect

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. Do you have defined cybersecurity incident escalation criteria, notifications, activations, and/or courses of action?
    a. If so, what actions would be taken at this point? By who?
    b. Would leadership be notified?
4. How does your organization baseline network activity? How would you be able to distinguish between normal and abnormal traffic?
5. Does the organization report cybersecurity incidents to outside organizations? If so, to whom? What, if any, mandatory reporting requirements do you have?
6. At what point would your organization begin to suspect the HVAC/Fire alarm issues might be the result of malicious cybersecurity activity?
7. If you were one of the individuals who received the email demanding bitcoin payment, who would you inform, internally? Who, if anyone would you inform externally?
8. Do detection and analysis procedures differ for loss of personally identifiable information (PII), phishing attempts, data exfiltration, data modification, or other incidents?
9. Would this be considered the most severe tier of security incident for your organization? What, if any, additional notifications or actions would this prompt?
10. Who is responsible for correlating information across different organizational-level incidents?
11. What resources and capabilities are available to analyze the intrusions:
    a. Internally?
    b. Externally though government partners?
    c. Through the private sector?
12. How is information shared among your internal and external stakeholders? Through formal or informal relationships? What information sharing mechanisms are in place?
13. Discuss your organization's intrusion detection capabilities and analytics that 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 (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")?
    e. What are the primary and contingency communication mechanisms necessary to support incident management?

2. Do you have someone within your organization who monitors the Dark Web? If so, how would you verify the security researcher's claims and confirm authenticity of the sensitive information in question?
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. Will IT alert authorities? Have your public relations priorities changed?
    b. Will it trigger any additional legal or regulatory notifications?
7. 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. Are you keeping senior leadership updated? What information is provided and how is it communicated?
    c. Would you make any notification to the public?
        i. If so, how are you coordinating your messaging within your organization?
        ii. Do you have pre-canned messaging or holding statements 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. Would any of these issues be considered a cyber incident at this point?
11. Do these incidents generate any concerns that have not been addressed?
12. How would your organization respond to the discovery of a malicious, unauthorized administrator account on your systems? Who would be informed internally? Who would be informed externally (e.g. law enforcement, cybersecurity insurance partners, etc.)?
13. What resources are required for incident investigation and attribution? Are sufficient resources available in-house?
14. Would the events presented in the scenario trigger activation of your emergency operations plan cyber incident annex? If so, would that alter any roles and responsibilities?
    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? Where is the process documented?
    c. How does a law enforcement investigation impact containment, eradication, and recovery efforts?
15. Are processes and resources in place for evidence preservation and collection?
16. Discuss the difference between network and host forensics. How are you equipped and staffed to address this?

17. Do you have a network operations center? Security operations center? What are their roles 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. Is there a way to 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? Are your current resources 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? How do you request these resources?
    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. Does this exceed your organization's ability to respond?
    a. If so, are there established procedures to request additional support?
22. What are your organization's response priorities?
    a. Who would be notified at this point in the scenario? Is there a plan in place detailing the thresholds at which different notifications are made and what information is provided?
    b. What response actions would the IT/IS department take at this point? Are these actions driven by a plan?
    c. What response capabilities and resources are required to respond to these incidents?
23. What actions would be taken when the exfiltration is discovered? Does your organization have written plans that would be implemented?
24. Do you pay the ransom?
    a. Who decides?
    b. What's the process?
    c. What are the advantages/disadvantages to paying?
    d. What are the political ramifications?
    e. What outside partners/entities do you need to contact?
25. Where do you receive cyber response technical assistance? Do you have plans, procedures or policies in place to access this assistance?
26. Have you proactively identified and established the service provider relationships needed 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?
    b. Is information flowing in both directions?
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. Would your organization engage in any post-incident activities?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
    a. Would senior leaders consider re-activating critical business processes and systems? What is the risk associated with doing so?
    b. Would your organization consider a complete rebuild of these systems? How long and costly would that process be?
    c. What factors do you consider when making these decisions?
3. What formal policies and procedures does your organization use to decide when and how to restore backed-up data, including measures for ensuring the integrity of backed-up data before restoration?
4. Does your organization have back-ups of vital records 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. Are redundant systems 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. Does your organization have a continuity of operations plan (COOP) for conducting its functions at a location other than your main building?
    a. If so, how would a suspected cyber incursion impact your organization's ability to activate its COOP Plan?
10. Are alternative systems or manual processes in place to continue operations if a critical system is unavailable for a significant period of time?
    a. Who can authorize use of alternate systems or procedures?

Training and Exercises

1. Does your organization provide basic cybersecurity and/or IT security awareness training to all users (including managers and senior executives)?
    a. How often is training provided? Does it cover:
        i. Review of department and/or agency acceptable use and IT policies,
        ii. Prominent cyber threat awareness,
        iii. Password procedures, and
        iv. Whom to contact and how to report suspicious activities?
    b. Is training required to obtain network access?
    c. What security-related training does your department or agency provide to, or contractually require of, IT personnel and vendors with access to your city's or county's information systems? How often do they receive the training?
2. Do your cybersecurity incident response team members undergo any special training to detect, analyze, and report this activity? If so, can you describe this training?

   a. Is your staff sufficiently 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?
   a. Do employees know what constitutes suspicious cybersecurity activities or incidents?
   b. Do they know what actions to take when one arises?
4. If you have a cyber incident response plan, how often does your organization exercise the plan?
   a. Who is responsible for the exercise planning?
   b. What agencies are involved in the exercise?
   c. What level of the organization is required to participate?
   d. What actions follow the exercise?
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. Do your organization's exercise efforts include both physical and cyber risks?
8. Have senior or elected officials participated in a cybersecurity exercise?
9. Are there additional training and/or exercising requirements for your organization?

Senior Leaders and Elected Officials

1. What is your cybersecurity culture? As a leader in your organization, what cybersecurity goals have you set? How have they been communicated?
2. As it relates to your jurisdiction, what cybersecurity information do you request? What do you receive?
3. What are your cybersecurity risks?
4. Who develops your jurisdiction's cybersecurity risk profile? What are their reporting requirements? Are they directed to, required by statute, or other? How often do they report?
5. Is your cybersecurity risk integrated with physical risk for an integrated jurisdictional risk assessment?
6. What is your jurisdiction's greatest cybersecurity concern? Why do you rate this concern as your greatest concern? Who reports to you on cyber threats?
7. What, if any, infrastructure does your jurisdiction own, operate, and/or regulate?
8. What relationships do you have with critical infrastructure owners and operators?
9. What priorities have you set related to the cybersecurity of critical infrastructure?
10. What is your most important critical infrastructure?
11. What are your regulatory requirements related to critical infrastructure, if any?
12. What is the greatest threat facing your critical infrastructure? What, if anything, is your jurisdiction able to do to mitigate it?
13. When did you last receive a cyber threat briefing for your jurisdiction?
14. How has your jurisdiction prepared for a cyber incident?
   a. Does your jurisdiction have cybersecurity plans in place? How many information security officers do you have?
   b. Does the plan indicate how they will work together?
15. Have your information security officers and emergency managers jointly planned for cybersecurity incidents?
16. What are your cybersecurity workforce gaps? How does your jurisdiction recruit, develop, and retain cybersecurity staff?

17. What cybersecurity training do you have planned for cybersecurity staff, managers, and general workforce?
18. What magnitude of incident would require your notification? How does that notification process work? Is it planned?
19. What requirements or agreements, if any, exist for critical infrastructure to notify you of a cyber incident?
20. Who advises you on cyber threats? What are your essential elements of information or critical information requirements?
21. What is your planned role in protective action decision-making?
22. What is your planned cyber incident management structure? What parts of the government need to be engaged?
23. Would your jurisdiction's Emergency Operations Center be activated in a cyber incident? How? Why?
24. What is your role in a cyber incident?
25. How does a law enforcement investigation impact your response?
26. What is your role in communicating to the public?
27. How are costs of the response calculated?
28. What information do you need to support your decision-making process?
29. Who is your jurisdiction's cybersecurity liaison to privately-owned and operated critical infrastructure?
30. What are your expectations of the State and Federal Government?
31. Describe your role in post-incident activity.
32. What is your role in restoring and/or maintaining public confidence?

Media

1. What are your public affairs concerns? Who is responsible for coordinating the public message? Is this process a part of any established plan?
    a. How would your department respond to the local media reports?
    b. What information are you sharing with citizens? Employees?
    c. Are public information personnel trained to manage messaging related to cyber incidents?
    d. Does your department have pre-drafted statements in place to respond to media outlets?
    e. Are they trained to manage your social media presence?
    f. Are all personnel trained to report any contact with the media to appropriate public information personnel?
2. What information would your organization communicate to the public?
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. Does your state have security breach notification laws? If so, what do they include?

Appendix B: Acronyms

Acronym	Definition
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
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
TA	Technical Alert
TLP	Traffic Light Protocol

Appendix C: Case Studies

Emotet Malware Infection

As of July 30, 2018, a multi-pronged, zero-day attack affected Matanuska-Susitna Borough, Alaska[1], forcing a declared disaster that crippled the borough's computer infrastructure, including servers, telephones, and email exchange. According to Matanuska-Susitna Borough's IT Director, components of the attack included the Emotet Trojan, BitPaymer ransomware, and an actual hacker logging into the borough's network. Some of the malware was dormant on the borough's computers since as early as May 3, 2018. Overall, nearly all of the borough's 500 workstations and 120 out of 150 servers were affected.

In another example, nearly 3,000 patients of the Oregon Endodontic Group had their dates of birth, diagnoses, treatments, and health insurance data exposed[2] after an email account was infected with Emotet malware. About 41 patients saw their Social Security number exposed, while seven patients had financial data breached and two had their driver's licenses exposed. The Emotet breach marked the third significant breach of Minnesota-based Healthcare entities in the span of a year.

Distributed Denial of Service Attack

On February 28, 2018, GitHub, a popular developer platform, was hit[3] with a flood of record-breaking traffic that clocked in at 1.35 terabits per second. According to GitHub, the traffic was traced back to over a thousand different autonomous systems (ASNs) across tens of thousands of unique endpoints.

Social Engineering

UnityPoint Health experienced the largest U.S. breach in 2018, as the records of 1.4 million patients were compromised by a phishing attack that gave hackers access to internal email accounts[4]. The investigation found that the hackers were likely trying to use the email system to divert vendor or payroll payments. However, officials stated that the electronic health record (EHR) and billing systems weren't impacted by the attack. The hacked accounts included protected health information and, for some of the 1.4 million patients, payment card and social security numbers. As a result of the attack, UnityPoint reset the passwords on the compromised accounts, conducted mandatory phishing education for employees, added security tools to identify suspicious emails, and implemented multi-factor authentication.

Ransomware

On May 12, 2018, one of the most notorious ransomware attacks began affecting systems across the globe. Experts estimate more than 300,000 systems have been affected by the variant known as WannaCry across the globe. A common way for this ransomware to spread is through standard file sharing technology, i.e. through vulnerabilities in Microsoft Windows Server Message Block (SMB). The vulnerability used in this attack was exploited to drop a file on the vulnerable system and then

[1] (Sullivan, 2018)
[2] (Davis, Minnesota DHS Reports Health Data Breach from 2018 Email Hack, 2019)
[3] (Kottler, 2018)
[4] (Davis, 1.4 million patient records breached in UnityPoint Health phishing attack, 2018)

executed as a service, encrypting files (commonly used by Microsoft Office, databases, file archives, multimedia files, and various programming languages) with the *.WNCRY* extension[5].

In 2019, WannaCry continued to affect many organizations, particularly in the healthcare and manufacturing sectors. According to a research report from internet of things security company, Armis, WannaCry continues to be an active threat. Armis claims WannaCry was "reportedly responsible for 30% of all ransomware attacks worldwide in Q3 2018, and over 145,000 devices worldwide are still compromised".[6]

[5] (Symantec Threat Intelligence, 2017)
[6] ("Wannacry Two Years Later: How Did We Get The Data?", 2019)

Appendix D: Attacks and Facts

Distributed Denial of Service

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

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

Additional Resources

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

Social Engineering

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering–the manipulation of users through human interaction and the formation of trust and confidence to compromise proprietary information. Techniques for uncovering this information largely involve the use of phishing, i.e. email or malicious websites that solicit personal information by posing as a trustworthy source. Social engineering is effective for breaching networks, evading intrusion detection systems without leaving a log trail, and is completely operating system platform dependent. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the human factor. Organizations should take steps towards strengthening employee cybersecurity awareness training, to include training personnel to be cautious of suspicious emails, know where to forward them and keeping software and systems up-to-date.

Additional Resources

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

Ransomware

Ransomware is a type of malware that denies access to victims' data or systems through encryption with a key only known by the malicious actor who deployed the malware. Once encrypted, the ransomware directs the victim to pay the attacker, typically in the form of cryptocurrency, so the victim can receive a decryption key. Ransomware typically spreads through phishing emails or by

unknowingly visiting an infected website. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

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

Appendix E: Doctrine and Resources

Laws

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

Presidential Directives

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

Strategies and Frameworks

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

Key Points of Contact

- Department of Homeland Security/Cybersecurity and Infrastructure Security Agency (CISA) (contact: central@cisa.dhs.gov)
- Federal Bureau of Investigation (FBI)
    - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
    - Internet Crime Complain Center (IC3) (contact: http://www.ic3.gov)
- National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: cywatch@ic.fbi.gov; (855) 292-3937)
- United States Secret Service Field Offices and Electronic Crimes Task Force (ECTFs) (contact: https://www.secretservice.gov/contact/field-offices/)

Other Available Resources

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

References Cited

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

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

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

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

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

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

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

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

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