CISA Tabletop Exercise Package Ransomware

[Enter Organization Name]

<Exercise Date>

Updated June 2024

Cybersecurity and Infrastructure Security Agency

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 Activities	**Time**	**Activity**
	20 Minutes	Threat Briefing and Opening Remarks
	60 Minutes	Module 1
	20 Minutes	Break
	60 Minutes	Module 2
	20 Minutes	Hotwash
Purpose	Examine the cyber resilience of <Organization> in response to a significant cyber incident.	
National Institute of Standards and Technology Cybersecurity Framework	Govern, Identify, Protect, Detect, Respond, Recover	
Objectives	1. Examine the response capabilities of <Organization> during a significant cyber incident. 2. Evaluate the ability for <Organization> to coordinate information sharing during a significant cyber incident. 3. Identify areas of improvement in cyber incident response plans and overall organizational resilience during and following a significant cyber incident. 4. Explore <Organization>'s plans to recover and restore services, mission critical assets, or systems.	
Threat or Hazard	Ransomware	
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) 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 Information	CISA National Cyber Exercise Program (NCEP) cisa.exercises@cisa.dhs.gov

General Information

Building Resilience

The purpose of the National Cyber Exercise Program's CISA Tabletop Exercise Packages (CTEPs) are to increase your organization's resilience by assessing and validating capabilities and identifying areas for improvement. The National Institute of Standards and Technology (NIST) defines cyber resilience as "the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources."[1]

Using this Situation Manual

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. There are footnotes with corresponding resources throughout the modules to guide your preparedness efforts. The appendices provide the following information to tailor the exercise discussion:

- Appendix A: Additional discussion questions that can replace or augment the existing Module 1 and 2 discussion questions.
- Appendix B: Reference section for acronyms used within this situation manual.
- Appendix C: Case studies that provide real-world examples of the threats presented in this scenario.
- Appendix D: An explanation of the threats presented in this scenario.
- Appendix E: Additional cybersecurity preparedness and response resources.

Participant Roles and Responsibilities

Players have an active role in discussing or performing their primary roles and responsibilities during the exercise. Players discuss or initiate actions in response to the scenario.

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.

[1] National Institute of Standards and Technology, "Computer Security Resource Center Glossary: Cyber Resilience," https://csrc.nist.gov/glossary/term/cyber_resiliency.

Exercise Structure

This exercise is intended to 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, including a CISA cyber threat alert release, 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 PII, and execution of ransomware.
- Hotwash
- ***Structure Note:*** *Modules, timeline dates, and discussion questions included in each module may be modified as desired. Additional discussion questions for each module can be found in Appendix A.*

Exercise Guidelines

- This exercise is intended to be held in an open, no-fault environment. Varying viewpoints are expected.
- Respond to the scenario utilizing your knowledge of existing plans and capabilities, along with the valuable insights derived from your training and experience.
- Decisions are not precedent-setting and may not reflect your organization's final position on a given issue. This exercise is an opportunity to discuss and present multiple options, possible solutions, and suggested actions to resolve or mitigate a problem.
- There is no hidden agenda, and there are no trick questions. The resources and written materials provided are the basis for discussion. In any exercise, assumptions and artificialities are necessary to complete play within the given time, achieve training objectives, and account for logistical limitations. Please do not allow these factors to negatively impact your participation in the exercise.

Exercise Hotwash and Evaluation

The facilitator will lead a hotwash with participants at the end of the exercise to address any ideas or issues that emerge from the exercise discussions. The hotwash is held at the end of the exercise discussion. The hotwash is designed to provide an opportunity to discuss strengths and areas for improvement immediately following the conduct of an exercise.[2]

[2] FEMA, "Homeland Security Exercise and Evaluation Program," January 2020, https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

Module 1

Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) issues an Alert[3] regarding a new ransomware variant. This ransomware is being used in a campaign targeting state, local, tribal, and territorial governments, as well as private sector firms.

Day 2

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.[4] The final security patch was installed last week. This vulnerability was identified in your recently completed annual risk assessment.[5]

Day 4

An employee informs their manager that their work laptop was stolen from their car overnight. The laptop contained sensitive organizational information.[6]

Day 6

Members of your <Finance> department receive an email that appears to be from the Vice President of <Finance>. It instructs them to access a PDF containing details about an unpaid bill from a third-party vendor supporting your organization. Several employees call the Vice President to verify the email's authenticity. She replies that she did not send it, and that there is no outstanding vendor bill. Nevertheless, some employees still open the PDF.[7]

Discussion Questions

Discussion questions included in each module are designed to explore different aspects of your operational resilience. The questions may be modified as desired. Additional questions can be found in Appendix A.

1. What are the greatest cyber threats to your organization?
2. What information technology (IT) systems or processes are the most critical to your organization?
3. What cybersecurity threat information does your organization receive?
    a. What cyber threat information is most useful?
    b. How is information disseminated across your organization and by whom?
    c. What actions would your organization take following an alert like the one presented in the scenario?

---

[3] CISA Cybersecurity Alerts & Advisories, https://www.cisa.gov/news-events/cybersecurity-advisories.
[4] NIST CSF 2.0 via CPRT, "GV.SC-07: The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship CPG Checklist," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC-07.
[5] NIST CSF 2.0 via CPRT, "Data Security," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS.
[6] NIST CSF 2.0 via CPRT, "PR.AT-01: Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AT-01.
[7] CISA CPG Checklist, "2.I Basic Cybersecurity Training [PR.AT-1]," https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist.

4. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?
    a. What information technology (IT) systems or processes are the most critical to your organization?
    b. Describe your organization's asset management plan and how you prioritize critical assets.
    c. What improvements have been implemented to enhance cyber resilience following recent risk assessments?
    d. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?
5. Does your organization have backups of vital records stored in a location separate from your primary working files/copies?
    a. How frequently do you run backups?
    b. How long do you keep copies of archived files backed up?
    c. How long would it take to restore primary files from backups?
6. Discuss your risk management strategy.
    a. How is it developed/maintained?
    b. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?[8]
    c. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
7. Describe your organization's cybersecurity training program for employees.
    a. How often are employees required to complete this training?
    b. Is training required during employee onboarding before granting system/network access?
    c. What additional training is required for employees who have system administrator-level privileges?
    d. What type of training methods or approaches have you found most beneficial?
8. How do employees report suspected phishing attempts or other possible cybersecurity incidents?
    a. What actions does the IT department take when suspicious emails are reported?
    b. What feedback do employees receive after reporting a suspicious email or event?

[8] CISA Resources, "Zero Trust Maturity Model," https://www.cisa.gov/zero-trust-maturity-model.

Module 2

Day 7

An increase in Domain Name System (DNS) traffic outside of standard business hours is flagged by your organization's intrusion detection system and an alert is sent to your <IT team/Security Operations Center>.[9] Upon further investigation of the system logs, they discover that a significant amount of data was sent from known HR employee IP addresses to external IP addresses.[10]

Day 9

Computers throughout your organization 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.[11]

Day 10

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 gained access to PII, including <employee social security numbers, bank account and routing number information, etc.>. The hacker group shared a limited number of data records to substantiate their claims and assert their intention to sell the data.[12]

Day 11

News outlets report on the cyber incident. Several news outlets contact your organization for comments on the ransomware infection and data breach.

Discussion Questions

1. Discuss your organization's cyber resilience planning.
    a. What information technology (IT) infrastructure has been identified to support mission essential functions in continuity of operations and incident response plans?
    b. How has your organization prioritized IT infrastructure for restoration?
    c. How has cybersecurity been integrated into your continuity plans?
2. How does your organization baseline network activity?[13]
    a. How can you distinguish between normal and abnormal traffic?

---

[9] NIST CSF 2.0 via CPRT, "PR.PS-04: Log records are generated and made available for continuous monitoring," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.PS-04.
[10] NIST CSF 2.0 via CPRT, "DE.CM: Continuous Monitoring" https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM.
[11] NIST CSF 2.0 via CPRT, "DE.CM-09: Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=DE.CM-09.
[12] NIST CSF 2.0 via CPRT, "PR.DS-01:The confidentiality, integrity, and availability of data-at-rest are protected," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS-01.
[13] NIST CSF 2.0 via CPRT, "PR.IR-03: Mechanisms are implemented to achieve resilience requirements in normal and adverse situations," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.IR-03.

3. Utilizing your organization's cyber incident response plan (CIRP), describe the actions that your organization would take at this time.
    a. Describe the training your employees receive on this plan.
    b. What guidance does the plan include on assessing the severity of the incident?
    c. How does incident severity level dictate response?[14]
    d. How are critical systems and processes incorporated within your CIRP?
4. What redundant systems exist for when primary systems are compromised?
    a. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
    b. Who can authorize use of alternate systems or procedures?
    c. How long can you perform manual or alternate processes on your critical systems?
5. What security breach notification laws does your state or industry have?
6. Explain your organization's decision-making process regarding ransomware payment.[15]
    a. Are ransomware policies/procedures included in your CIRP?
    b. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
    c. Discuss the advantages and disadvantages of either agreeing or refusing to pay.
    d. Describe the impact the sale or release of sensitive information or PII would have on your response and recovery activities.
    e. Discuss potential legal and reputational ramifications of paying or not paying the ransom.
7. What capabilities and resources are required for responding to this scenario?[16]
    a. What additional resources outside of your organization would be necessary for responding to the cyber incident?
    b. What are the processes or procedures for requesting additional resources?
    c. What external partners (e.g., CISA, FBI, etc.) would you contact for assistance?
8. Describe your organizational processes to respond to the media reports and inquiries.
    a. What pre-scripted messages have been developed for cyber incidents?
    b. What training do your communications personnel receive on cyber terminology?
    c. How would public messaging be coordinated and disseminated during a cyber incident?
    d. How would you preserve and reinforce the public's confidence and trust in your organization during a significant cyber incident?
9. Based on discussion, what changes would you implement to increase the resilience of your organization?

---

[14] NIST CSF 2.0 via CPRT, "ID.IM-04: Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?keyword=incident%20response%20plan

[15] CISA, "Stop Ransomware," https://www.cisa.gov/stopransomware.

[16] NIST CSF 2.0 via CPRT, "GV.OV: Oversight," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.OV.

Appendix A: Additional Discussion Questions

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

Cyber Resilience

1. Discuss how cyber preparedness has been integrated with your current all-hazards preparedness efforts.
2. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
    a. What were the most recent results and action items that followed?
3. Describe your organization's review process for your CIRP.
    a. How often is the CIRP reviewed?
    b. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
    c. How are updates to the plan communicated to department or agency employees?
4. Discuss your supply chain concerns related to cybersecurity infrastructure.
5. What cybersecurity language is included within third-party vendor contracts?
    a. How do you evaluate the cybersecurity posture of your vendors?
    b. How often are contracts reviewed?
    c. How do your service level agreements address cyber incident notification?
6. What level of access do your third-party vendors have to your organization's network?
    a. What mechanisms or processes are in place to prevent malicious activity?
7. Describe your IT department's patch management plan.
    a. What risk assessments have been performed on network servers?
    b. What processes are in place to proactively evaluate each server's criticality and applicability to software patches?
    c. What considerations are addressed in the plan's risk management strategy? (e.g., extended downtime, loss of data, impaired functionality, etc.)
8. What is your method for tracking and identifying firmware vulnerabilities in your organization's network?
9. How would these scenario events affect your organization's business operations/processes?
10. How are IT and business continuity functions coordinated with physical security?
11. What processes do you have to ensure that your external dependencies are integrated into your security and continuity planning programs? (e.g., contractors, power, water, etc.)
12. How is the integrity of your critical data protected and validated?
    a. What external entities have access to the database?
    b. How would those entities report a breach of their systems to your office?

13. What is your cyber incident management structure?
    a. Who leads incident management and why?
    b. How are they notified?
    c. How often are roles and responsibilities within this structure exercised with employees?
14. What mission essential functions are impacted by the incidents described in the scenario?
15. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?
16. What mechanisms (e.g., Memorandum of Understanding (MOU)/Memorandum of Agreement (MOA), contract, etc.) are in place for arranging additional surge support of both personnel and resources if needed?
17. If primary communications are compromised, how do you provide information to internal and external entities?
18. What policies and procedures does your organization use to decide when and how to restore backed-up data?
    a. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?

Employee Accounts & Privileges

1. Describe your organization's employee off-boarding process.
    a. Is this process coordinated with Information Technology (IT) and Human Resources (HR)?
    b. What additional actions are taken if the employee's termination is contentious?
    c. How does your organization retrieve all information system-related property during the employment termination process (e.g., authentication key, system administration's handbook/manual, keys, identification cards, etc.)?
2. Describe your organization's bring your own device (BYOD) policy.
3. What are your organization's policies or procedures for IT account management?
    a. What are the protocols for establishing, activating, modifying, disabling, and removing accounts?

Incident Identification

1. How are cyber incidents reported within your organization?
    a. What would trigger the reporting requirements established by regulation, state law, and/or organization policy?
    b. What training have employees received regarding reporting requirements and your cyber incident response plan?
2. What cybersecurity incident escalation criteria is defined in your cyber incident response plan?
    a. Who would be responsible and what actions would they take based on the scenario?
    b. Who would need to be notified internally and externally according to the plan?
    c. When would leadership be notified?

3. Discuss your organization's intrusion detection capabilities and analytics that alert you to a potential cyber incident.
    a. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
4. Describe your organization's ability to monitor the Dark Web.
5. How often is your organization's data reviewed? How would you determine whether unauthorized manipulation of data has occurred?

Incident Response

1. What are your processes for collecting evidence and maintaining the chain of custody during a cyber incident?
2. What additional concerns have the incidents described in this scenario generated that have not been addressed in today's discussion?
3. At what point in the scenario would you contact law enforcement?
    a. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
    b. What are the processes and resources for evidence preservation and collection?
4. What are the roles of your network operations center and security operations center during a response?
5. What are the processes for contacting critical personnel outside of core hours?
    a. How do you proceed if critical personnel are unreachable or unavailable?
6. How would a breach of vendor(s) affect your organization if they potentially have access to your information?
    a. What are the notification requirements to your organization for breaches?
7. Who is responsible for coordinating information across different organizational-level incidents?

Recovery

1. When does your organization determine a cyber incident is over?
    a. Who makes this decision?
    b. What post-incident activities would your organization conduct?
2. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
    a. What is the risk associated with re-activating critical business processes and systems?
    b. How long and costly would the process be to completely rebuild these systems?
    c. What factors do you consider when making these decisions?

Training & Exercises

1. What training does your cybersecurity incident response team undergo to detect, analyze, and report malicious activity?
    a. What additional training and/or exercise requirements do you require for your incident response staff?

2. How often does your organization exercise its CIRP?
    a. What agencies are involved in the exercise?
    b. What level of the organization is required to participate?
3. How does your organization's training and exercise efforts address both physical and cyber risks?
    a. Have senior staff participated in a cybersecurity exercise?

Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
    a. How do these goals align with organizational objectives?
2. What critical infrastructure does your organization own, operate, and/or regulate?
    a. What critical infrastructure is most important to your organization for continuing operations?
    b. What relationships do you have with critical infrastructure owners and operators?
    c. What priorities and/or regulatory requirements have been set related to the cybersecurity of critical infrastructure?
3. What cybersecurity training is required for senior leadership?
4. At what point would you activate your organization's Emergency Operations Center?
5. What is your role during a cyber incident?
    a. What information do you need to support your decision-making process?
6. What are the gaps in your cybersecurity workforce?
    a. How does your organization recruit, develop, and retain cybersecurity staff?

Public Information

1. What information are you sharing internally (e.g., employees, leadership)?
2. What information are you sharing externally (e.g., residents, customers, vendors)?
3. What training are employees given on reporting any contact with the media to the appropriate public information personnel?
4. How do you build and maintain trust with your <customers/constituents>?

Legal

1. What is the role of the legal department during a cyber incident?
    a. What issues need to be addressed based on the scenario?
2. What legal documents should your organization have for cyber incidents?

Appendix B: Acronyms

Acronym	Definition
CIO	Chief Information Officer
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
COOP	Continuity of Operations Plan
CPG	Cybersecurity Performance Goals
BYOD	Bring Your Own Device
DDoS	Distributed Denial of Service
DHS	U.S. Department of Homeland Security
DNS	Domain Name System
EMS	Emergency Medical Services
FBI	Federal Bureau of Investigation
HR	Human Resources
IS	Information Systems
IT	Information Technology
MFA	Multifactor Authentication
MOA/MOU	Memorandum of Agreement/Memorandum of Understanding
NGO	Non-government Organization
NIST	National Institute of Standards and Technology
PHI	Protected Health Information
PII	Personally Identifiable Information
TLP	Traffic Light Protocol
ZTA	Zero Trust Architecture

Appendix C: Case Studies

Ransomware Attack Against US County

In January 2022, a large county in the United States experienced a ransomware attack that took office computers and several department websites offline. This led to the closure of county offices for several days, during which the sheriff's department and Emergency Medical Services (EMS) relied on backup contingencies.[17] Notably, due to the ransomware attack, the local detention center lost access to its automated door and camera systems. Adding to the impact, a sum of $191,000 worth of employee laptops was reported as damaged.[18]

County representatives declared their decision not to pay the ransom demands. Instead, they utilized their cyber insurance coverage to aid in recovery processes.[19] Subsequently, the county's Chief Information Officer (CIO) announced the implementation of multifactor authentication (MFA) for all users, aiming to enhance security controls. In response to the incident, the county commission purchased a new cybersecurity policy.

Ransomware Attack Against Chip Manufacturer

In early 2022, a computer chip manufacturer experienced a data breach followed by a subsequent ransomware attack. The company verified that the threat actors had leaked credentials of approximately 70,000 employees, along with proprietary company information.[20] As a result of this breach, the chipmaker's internal systems were compromised, leading to a two-day halt in multiple business operations.

The ransomware group Lapsus$ claimed responsibility for the attack and demanded a ransom of $1 million. In addition to the financial demand, the ransomware group also required the chipmaker to optimize their video cards to simplify cryptocurrency mining.[21] In response, the chipmaker took proactive steps to enhance their network security and partnered with experts specializing in cyber incident response.[22]

Malware Infection

On an early morning in February 2022, a satellite telecommunications provider experienced the beginning of a multifaceted cyberattack.[23] The incident began with a targeted distributed denial of service (DDoS) attack from company-provided consumer equipment, followed by thousands of modems going offline due to a malicious software. The malware was designed to systematically

---

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

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

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

[20] "5 Major Ransomware Attacks of 2022," *Cyber Management Alliance*, June 15, 2022, https://www.cm-alliance.com/cybersecurity-blog/5-major-ransomware-attacks-of-2022.

[21] Josephine Wolff, "A Tech Company Made It Harder to Use Its Products to Mine Crypto. Then Came the Ransomware Attack," *Slate,* March 30, 2022, https://slate.com/technology/2022/03/nvidia-gpus-cryptomining-ransomware-lapsususd.html.

[22] Pieter Arntz, "Nvidia, the ransomware breach with some plot twists," *Malware Bytes,* March 3, 2022, https://www.malwarebytes.com/blog/news/2022/03/nvidia-the-ransomware-breach-with-some-plot-twists.

[23] "KA-SAT Network cyber-attack overview," Viasat, March 30, 2022, https://www.viasat.com/about/newsroom/blog/ka-sat-network-cyber-attack-overview/.

delete essential files on UNIX operating systems, such as the ones used by this provider's modems. Once critical data was eradicated, the malware would initiate a device reset, rendering the modems unusable until restored to factory settings.

A forensic investigation led by the telecommunications provider revealed that the malware had been activated through "a legitimate management command," which was sent by a malicious actor with unauthorized access to their network. Thousands of customers temporarily lost their internet connection during the cyberattack. In response to the attack, the provider began shipping nearly 30,000 functional modems out to the affected customers, likely incurring further financial costs.

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 emails sent to employees.[24] 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 PII and protected health information (PHI) of nearly 500,000 employees, patients, and students may have been compromised.[25] This information included 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.

Credential and Information Theft

In August 2023, Microsoft Threat Intelligence reported that a Russian state-sponsored threat actor, Midnight Blizzard (previously tracked as NOBELIUM and APT29), had carried out highly targeted social engineering attacks utilizing credential theft phishing lures, which were sent as Microsoft Teams chat requests. Midnight Blizzard's campaign impacted nearly 40 global organizations, primarily within government, non-government organizations (NGOs), IT services, technology, discrete manufacturing, and media sectors. [26]

According to the Microsoft threat update[27], the hacker group impersonated technical support or a security team, sending a chat request to employees through Microsoft Teams. If the targeted employee accepted the request, they were prompted to authenticate via the Microsoft Authenticator application, providing the threat actor with access to the user's credentials. Victims confirmed instances of information theft from compromised domains.

The Microsoft threat update mentioned that Microsoft "mitigated the actor from utilizing the domains and continues to investigate this activity and work towards remediating the impact of the attack. (MS

---

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

[25] Mike Freeman, "UC San Diego Health sued over data breach that may have exposed records of 500,000 patients," *San Diego Union-Tribune*, September 24, 2021, 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.

[26] Z.Siddiqui, "Microsoft says Russia-linked hackers behind dozens of Teams phishing attacks," Reuters, August 2, 2023. https://www.reuters.com/technology/microsoft-says-russia-linked-hackers-behind-dozens-teams-phishing-attacks-2023-08-03/

[27] Microsoft Security "Midnight Blizzard conducts targeted social engineering over Microsoft Teams," https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams/

Security, 2023)" Microsoft urged organizations and users to remain vigilant against these advanced phishing schemes and to exercise caution when dealing with requests from external domains.

Appendix D: Attacks and Threats

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. Ransomware and associated data breach incidents can severely impact business processes, leaving organizations unable to access data necessary to function. The economic and reputational impacts of ransomware and data extortion have proven challenging and costly for organizations of all sizes throughout the initial disruption and, at times, extended recovery. Recovery can be an arduous process and there is no guarantee the victim will receive access to their data or systems if the ransom is paid. For more information on best practices to protect users from the threat of ransomware, as well as recent Alerts on specific ransomware threats, see the resource list below.

Additional Resources

- CISA Stop Ransomware Website (https://www.cisa.gov/stopransomware)
- CISA Stop Ransomware Guide (https://www.cisa.gov/resources-tools/resources/stopransomware-guide)
- Protecting Against Ransomware (https://www.cisa.gov/news-events/news/protecting-against-ransomware)

Social Engineering and Phishing

One of the most prominent tactics attackers use to exploit network and system vulnerabilities is social engineering, which is 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 and evading intrusion detection systems without leaving a log trail, and it is completely dependent on the operating system platform. While technical exploits aim to bypass security software, social engineering exploits are more difficult to guard against due to the involvement of human emotions. Organizations should take steps towards strengthening employee cybersecurity awareness training by incorporating trainings on identifying suspicious emails, instructing personnel on how to report them, and emphasizing the importance of keeping software systems up to date.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks)
- Phishing (https://www.nist.gov/itl/smallbusinesscyber/guidance-topic/phishing)

Appendix E: Contacts and Resources

Federal Government Resources

- CISA (contact: central@cisa.gov, https://www.cisa.gov)
- United States Secret Service (USSS) Field Offices and Electronic Crimes Task Forces (ECTFs) (contact https://www.secretservice.gov/contact/field-offices, https://www.secretservice.gov/investigation/cyber)
- Federal Bureau of Investigation (FBI)
  - Field Office Cyber Task Forces (contact: https://www.fbi.gov/contact-us/field-offices)
  - Internet Crime 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)

State Level Resources

- Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: info@msisac.org; 518-266-3460)
- National Governors Association (NGA) (https://www.nga.org/)
  - NGA Center for Best Practices (https://www.nga.org/bestpractices/divisions/hsps/)
- DHS Cybersecurity Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)
- National Association of State Chief Information Officers (NASCIO) (https://www.nascio.org/)

Private Sector/Business Resources

- InfraGard (https://www.infragard.org/Files/InfraGard_Redesign_2-24-2022.pdf)
- Internet Security Alliance (https://isalliance.org/)
- Information Sharing and Analysis Centers (ISACs) and Information Sharing and Analysis Organizations (ISAOs) (https://www.isao.org/information-sharing-groups/)
  - International Association of Certified ISAOs (http://www.certifiedisao.org; contact: operations@certifiedisao.org)
  - National Council of ISACs (https://www.nationalisacs.org)

Preparedness Resources

- CISA Cross-sector Cybersecurity Performance Goals (https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist)
- NIST Cybersecurity Framework Tools (https://www.nist.gov/cyberframework)