CISA Tabletop Exercise Package
Supply Chain/Vendor Compromise

[Enter Organization Name]

<Exercise Date>

Updated August 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

Handling Instructions 3
General Information 5
Exercise Overview 8
Module 1 9
Module 2 11
Appendix A: Additional Discussion Questions 13
Appendix B: Case Studies 16
Appendix C: Malicious Activity 18
Appendix D: Contacts and Resources 20
Appendix E: Acronyms 21

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>.

General Information

Building Resilience

The purpose of the National Cyber Exercise Program's (NCEP) CISA Tabletop Exercise Packages (CTEPs) is 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]

The CTEP materials (https://www.cisa.gov/resources-tools/services/cisa-tabletop-exercise-packages), including this Situation Manual, are designed to support the planning and execution of a tabletop exercise. A tabletop exercise is a discussion-based exercise in response to a scenario intended to generate a dialogue of various issues, identify strengths and areas for improvement, and/or achieve changes in perceptions about plans, policies, or procedures.[2] NCEP also offers facilitated CTEPs. If you are interested in NCEP assistance with the planning and execution of a facilitated CTEP, please contact cisa.exercises@cisa.dhs.gov.

Using this Situation Manual

This Situation Manual provides a scenario and accompanying discussion questions designed to identify strengths and areas for improvement, including understanding of plans, policies, and procedures. This Situation Manual is intended to be adaptable and editable.

Modules 1 and 2 contain the scenario injects and discussion questions you will use to conduct the exercise. The footnotes throughout the modules contain corresponding resources to guide your preparedness efforts, including the CISA Cross-Sector Cybersecurity Performance Goals (CPG). 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**: Case studies that provide real-world examples of the threats presented in this scenario.
- **Appendix C**: An explanation of the threats presented in this scenario.
- **Appendix D**: Additional cybersecurity preparedness and response resources.
- **Appendix E**: Reference section for acronyms used within this situation manual.

[1] "Computer Security Resource Center (CSRC) Glossary: Cyber Resilience," National Institute of Standards and Technology, accessed August 2, 2023, https://csrc.nist.gov/glossary/term/cyber_resiliency.
[2] "Homeland Security Exercise and Evaluation Program," FEMA, February 2020, https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep.

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. Players may include IT/information security personnel, emergency management personnel, human resources personnel, legal personnel, external partners, and any other personnel with a role in incident response.
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. Observers may include senior-level leadership, IT/information security personnel, emergency management personnel, legal personnel, external partners, and any other personnel without a role in incident response.
Facilitators provide situation updates and moderate discussions. They also provide additional information or resolve questions as required. Key Exercise Planning Team members may also assist with facilitation as subject matter experts during the exercise.
Note-takers are assigned to observe and document exercise activities. Their primary role is to document player discussions, including how and if those discussions conform to plans, policies, and procedures.

Exercise Structure

This exercise 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 a state of the world describing a global cybersecurity incident impacting Managed Service Providers (MSPs) and your organization acquiring a new MSP.
  - **Module 2:** This module covers the downstream impacts of a cyber incident at your MSP.
- 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 hotwash is a short meeting held immediately after the end of the exercise discussion/conduct. The facilitator will lead participants through a review of the exercise discussion, identifying strengths and areas for improvement. The hotwash is also an opportunity for evaluators to ask clarifying questions, as needed.[3]

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

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 impacting the supply chain. 2. Evaluate vulnerabilities associated with third-party vendor relationships. 3. Identify areas for improvement in cyber incident response plans and overall organizational resilience during and following a significant cyber incident.	
Threat or Hazard	Cyber incident	
Scenario	Your organization's Managed Service Provider (MSP) is the victim of a cyber incident, leading to impacts on the managed services they provide to your organization.	
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

Module 1

Day 1

CISA and the Federal Bureau of Investigation (FBI) launch a joint response to a global cybersecurity incident in which malicious actors executed ransomware attacks against Managed Service Providers (MSPs) and their downstream customers. The malicious actors leveraged a vulnerability in a popular Remote Monitoring and Management (RMM) software.[4] Once the malware was discovered, the software was shut down. Impacted MSPs were unable to provide services to customers worldwide, affecting the critical functions of entities across sectors, including gas stations, pharmacies, railways, and public broadcasting. Your organization is not impacted at this time.

Discussion Questions

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

1. What are the greatest cyber threats to your organization?
    a. What are the possible impacts of an intrusion into your systems?
2. What cybersecurity threat information does your organization receive?
    a. What are your primary sources of information?
    b. How do you determine what information is relevant to your equipment and operations?
    c. What threat information is most useful?
    d. What actions would your organization take in response to a report like the one presented in the scenario?

Day 7

Your organization contracts a new MSP who is known as a trusted partner across your sector. Their platform is installed and updated with no alerts from your intrusion detection software.[5]

3. Has your organization conducted a risk assessment to identify specific cyber threats, vulnerabilities, and critical assets?[6]
    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. Do you use a cyber supply chain risk management (C-SCRM) approach to managing supply chain risk?[7]

---

[4] CISA "Cybersecurity Alerts and Advisories," https://www.cisa.gov/news-events/cybersecurity-advisories.
[5] CSF 2.0 via CPRT, "GV.SC: Cybersecurity Supply Chain Risk Management," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.SC.
[6] CSF 2.0 via CPRT, "GV.RM: Risk Management Strategy," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.RM.
[7] NIST Computer Security Division, Computer Security Resource Center, "Cyber Supply Chain Risk Management (C-SCRM)," https://csrc.nist.rip/scrm/.

   d. What improvements were implemented to enhance cyber resilience following recent risk assessments?
   e. Does your organization have a vulnerability management program dedicated to mitigating known exploited vulnerabilities in internet-facing systems?[8]

4. What is the role of cybersecurity in the review and selection of third-party vendor support?
   a. What cybersecurity language, (e.g., cybersecurity training and cyber incident notification requirements) is included within third-party vendor contracts?
   b. How do you evaluate the cybersecurity posture of your vendors?
   c. How often are contracts reviewed?
5. What level of access do your third-party vendors have to your organization's network?[9]
   a. How often are third-party access rights and data logs reviewed?

Day 8

Data from multiple sector partners is found on the DarkWeb. Some of these sector partners recommended your new MSP to you.

6. How is your network configured (e.g., network segmentation, least privilege access, etc.) to defend against malicious actors?
7. What tools (e.g., threat hunting, security audits, etc.) do you leverage as part of a proactive cybersecurity strategy?
8. What indicators of compromise feeds does your organization use?
9. What steps do you take to protect organizational data from data loss/theft?[10]
   a. What cybersecurity best practices do you leverage before giving access to sensitive business data?

Day 10

Your IT department authorizes the installation of a software update from your new MSP on one of your critical systems. The update will improve system functionality.[11]

10. Describe your organization's patch management and vulnerability management plans.
    a. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
    b. Describe your policies on remote access to your organization's network.
    c. What security protocols (encryption, etc.) exist on your hardware or software?

[8] CISA.gov, "Services: Vulnerability Scanning," https://www.cisa.gov/resources-tools/services/cisa-vulnerability-scanning.
[9] CSF 2.0 via CPRT, "PR.AA: Identity Management, Authentication, and Access Control," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.AA.
[10] CSF 2.0 via CPRT, "PR.DS: Data Security," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=PR.DS.
[11] CSF 2.0 via CPRT, "ID.RA-09: *The authenticity and integrity of hardware and software are assessed prior to acquisition and use*," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-09.

Module 2 – 6 months later

Day 182 - Morning

Employees at your organization are unable to sign in to the network when they arrive in the morning. Your IT helpdesk is inundated with calls reporting the issue. Your IT department contacts your MSP, but they are unable to reach the MSP <helpdesk/customer service representative>.

Day 182 - Afternoon

Employees are still unable to access your network. There are significant impacts to business-critical systems.

Discussion Questions

1. Using your organization's cyber incident response plan (CIRP)/continuity of operations plan, describe the actions your organization would take to minimize impacts on current operations.
    a. How does your plan define escalation criteria, notifications, activations, and/or courses of action?
    b. What guidance does the plan include for assessing the severity of the incident?
2. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
    a. Who can authorize the use of alternate systems or procedures?
    b. How long can you operate using manual processes or alternate systems when your primary critical systems fail?
    c. What additional staffing requirements are necessary for alternate systems or procedures, if any?

Day 182 – Evening

An independent cybersecurity company discovers your MSP was the victim of a cyber incident that impacted their widely used platform. The cybersecurity company suspects your MSP's customers unknowingly had malware on their system for up to two years. The company states any user of the MSP's platform could be affected by the malicious code, and recommends organizations take steps to identify and eradicate it.

3. How are third-party vendors involved in your incident response?
    a. How is this documented in your CIRP?
4. What does your service-level agreement include regarding incident response activity?

Day 185

The IT department starts an internal investigation. Their investigation discovers anomalous traffic in your network over the past seven months.

5. What capabilities and resources does your organization require in response to this scenario?
    a. What additional resources outside of your organization are 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?

6. What information are you sharing internally (e.g., employees, leadership)?
7. What information are you sharing externally (e.g., customers, partners, vendors)?
    a. What sector partners do you collaborate with before, during, and after a cyber-security incident?
8. 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?
9. Based on the discussion, what changes will you implement to increase the resilience of your organization against future attacks?[12]
    a. What measures will you take to better secure your network?

[12] CSF 2.0 via CPRT, "ID.IM: Improvement," https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.IM.

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 is integrated with your current all-hazards preparedness efforts.
2. What are the cybersecurity objectives for your organization?
    a. How do these align with your business objectives?
4. Describe your organization's review process for your CIRP.
    a. How is your CIRP integrated with other incident or emergency response/management plans?
    b. How often is the CIRP reviewed?
    c. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
    d. How are updates to the plan communicated to department or agency employees?
5. 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?
6. What is your method for tracking and identifying firmware vulnerabilities within your network?
7. How are IT and business continuity functions coordinated with physical security?
8. How is the integrity of your critical data protected and validated?
    a. What external entities have access to your data?
    b. How would those entities report a breach of their systems to your office?
9. What mission/business essential functions are impacted by the incidents described in the scenario?
10. How does your organization maintain availability of key assets (e.g., network connectivity, etc.)?

Accounts & Privileges

1. Describe your organization's "bring your own device" (BYOD) policy.
2. 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, law, and/or organization policy?
    b. What training do employees receive regarding reporting requirements and your CIRP?
2. 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 prevent and detect malicious activity on your systems/network?
3. How often is your organization's data reviewed?
    a. 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. At what point in the scenario would you contact law enforcement?
    b. How would a law enforcement investigation impact containment, eradication, and recovery efforts?

Recovery

1. When would your organization transition to the recovery and post-incident phases?
    a. How is the decision to transition to the recovery phase made?
    b. How does your organization conduct post-incident review?
    c. How are lessons learned/areas for improvement incorporated into process improvement planning (e.g., incident response plans, training, etc.)?
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 reactivating critical business processes and systems?
    b. How long and costly is the process 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. Who is involved in the exercises?
    b. What external agencies are involved in the exercises?
3. How does your organization's training and exercise efforts address both physical and cyber risks?

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. Describe your organization's cybersecurity culture.
3. What cybersecurity training is required for senior leadership?
4. At what point would you activate your organization's Security Operations Center/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 training do employees receive on reporting contact with the media?
2. How do you build and maintain trust with the public?

Legal

1. What is the role of the legal counsel during a cyber incident?
2. What internal legal guidance documents does your organization have for clients to use in planning for cyber incidents?
3. What are some examples of documents your legal counsel might provide legal review or assistance with drafting in response to a cyber incident?

Appendix B: Case Studies

Attack Against Software Used by MSPs Causes Major Downstream Impacts

A ransomware attack targeted a software provider used by numerous MSPs, causing significant downstream operational impacts in July 2021.[13] MSPs impacted by the breach managed various information technology for companies worldwide. The ransomware group exploited known vulnerabilities in the software provider's Virtual System Administrator (VSA), a remote monitoring and management software package, and deployed the ransomware to MSPs via the VSA software.[14]

The software provider received a ransom request of $70 million for an encryption key to unlock their system, while individual companies were presented with smaller tailored ransom amounts.[15] The far-reaching impacts included the closure of Swedish supermarket chain locations across the country for a week due to non-functioning cash registers. Some affected organizations chose to pay the ransom, while others, like the Swedish supermarket chain, did not. The software provider did not pay the $70 million ransom[16] and eventually obtained the decryption tool from an undisclosed third party to restore the encrypted data of impacted organizations.[17]

Ransomware Attack Against Vendor Impacts the UK's National Health Service

A ransomware attack on a software provider for the United Kingdom's National Health Service (NHS) led to delays in care and services provided by NHS for weeks.[18] The attack impacted systems for patient check-ins, medical notes, and the NHS 111 service. The affected systems were taken offline either by the LockBit 3.0 ransomware or as a precaution to avoid further damage.[4] Subsequently, the attacker moved laterally within the software provider's network, escalated their privileges, and deployed encryption malware.[19]

Double Supply Chain Compromise

In March 2023, a Voice over Internet Protocol (VoIP) software company discovered their systems were infiltrated. An employee of the VoIP company downloaded a malware-infected trading software application (app) onto their company computer. The advanced persistent threat (APT) group responsible for the compromises gained access to the VoIP company's systems with this app download. The APT then inserted malicious code into a component of the VoIP company's voice and video software suite, which according to the company, had over 600,000 customers with over 12

---

[13] Clare Duffy, "What we know about the Kaseya ransomware attack that hit hundreds of businesses," *CNN,* July 7, 2021, https://edition.cnn.com/2021/07/06/tech/kaseya-ransomware-what-we-know/index.html.

[14] Martin Giles, "Ransomware attacks sparked by cyberattack on kaseya," *Forbes,* July 3, 2021, https://www.forbes.com/sites/martingiles/2021/07/03/ransomware-attacks-sparked-by-cyberattack-on-kaseya/?sh=3fe7e4e92dab.

[15] Kari Paul, "Who's behind the Kaseya ransomware attack – and why is it so dangerous?" *The Guardian,* July 7, 2021, https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers.

[16] Joe Tidy, "Swedish Coop supermarkets shut due to US ransomware cyber-attack," *BBC,* July 3, 2021, https://www.bbc.com/news/technology-57707530.

[17] Kaseya, "Important Notice August 4th, 2021," https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-3rd-2021.

[18] Joe Tidy and Katharine da Costa, "Advanced cyber-attack: NHS doctors' paperwork piles up," *BBC,* August 30, 2022, https://www.bbc.com/news/technology-62725363.

[19] Michael Hill, "NHS ransomware attack fallout continues, services could be offline," *CSO Online*, September 1, 2022, https://www.csoonline.com/article/573567/nhs-ransomware-attack-fallout-continues-services-could-be-offline-for-another-12-weeks.html.

million daily users across multiple sectors.[20] The cyber threat actor gained control over the devices with the VoIP's desktop app installed, allowing them to download and execute code directly to client devices via a compromised version of the legitimate software. The malicious code downloaded a data extraction tool that tracked browser information.[21]

This incident was a double supply chain compromise, in which the compromise of the initial organization led the APT to obtain access to distribute malware into other organization's systems. After compromising the trading company, the APT was able to target their next victims, cryptocurrency firms.[22]

[20] Sergiu Gatlan, "3CX hack caused by trading software supply chain attack," *Bleeping Computer*, April 20, 2023, https://www.bleepingcomputer.com/news/security/3cx-hack-caused-by-trading-software-supply-chain-attack/.
[21] Jeff Johnson et al., Mandiant, "3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise," Mandiant, April 20, 2023, https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise.
[22] Sean Lyngaas, "North Korean hackers breach software firm in significant cyberattack," *CNN*, April 20, 2023, https://www.cnn.com/2023/04/20/politics/north-korea-hacking-supply-chain-3cx-mandiant/index.html.

Appendix C: Malicious Activity

Software Supply Chain Compromises

A software supply chain compromise occurs when a threat actor infiltrates a software vendor's network and employs malicious code to compromise the software. The vendor unknowingly sends the compromised software to its customers, which compromises their customer's data and/or system. Newly acquired software may be compromised from the outset, or a compromise may occur through other means like a patch or hotfix. In these cases, the compromise still occurs prior to the patch or hotfix entering the customer's network. These types of incidents affect all users of the compromised software and can have widespread consequences. To increase resilience against supply chain compromises, an organization should implement an enterprise-wide cybersecurity supply chain risk management (C-SCRM) approach. This approach includes managing critical components and suppliers, understanding the supply chain, collaborating with key suppliers, and including suppliers in resilience and improvement activities. For more information on supply chain risk management, see the resources listed below.

Additional Resources

- CISA Defending Against Software Supply Chain Attacks (https://www.cisa.gov/resources-tools/resources/defending-against-software-supply-chain-attacks)
- CISA Information and Communications Technology (ICT) Supply Chain Resource Library (https://www.cisa.gov/ict-supply-chain-resource-library)
- NIST Cybersecurity Supply Chain Risk Management Practices for Systems (https://csrc.nist.gov/pubs/sp/800/161/r1/final)

Social Engineering and Phishing

One of the most prominent tactics cyber threat actors use to exploit network and system vulnerabilities is social engineering, defined as the manipulation of users through human interaction in order to compromise proprietary information. Common social engineering techniques involve the use of phishing, vishing, and smishing. Phishing uses email and/or malicious websites to solicit personal information or to trick individuals into downloading malicious software. Vishing uses voice communication to convince a victim to share sensitive information. Advanced vishing incidents can take place completely over voice communications by exploiting Voice over Internet Protocol (VoIP) solutions and broadcasting services. VoIP easily allows caller identity to be spoofed. Smishing uses SMS/text messages to send malicious links, email addresses, and phone numbers.

Social engineering is effective for compromising networks and evading intrusion detection systems without leaving a log trail. 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, including training personnel to be cautious of suspicious emails, providing instruction on where to forward them, and keeping software and systems up to date. Organizations can also implement software designed to safeguard sensitive information, detect unsafe URLs, block phishing websites, detect known phishing and malware, and implement Multi-Factor Authentication (MFA) to guard against the use of stolen credentials.

Additional Resources

- Avoiding Social Engineering and Phishing Attacks (https://www.cisa.gov/news-events/news/avoiding-social-engineering-and-phishing-attacks)
- Phishing Guidance: Stopping the Attack Cycle at Phase One (https://www.cisa.gov/resources-tools/resources/phishing-guidance-stopping-attack-cycle-phase-one)

Appendix D: 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)
- DHS Fusion Centers (https://www.dhs.gov/state-and-major-urban-area-fusion-centers)

Preparedness Resources

- CISA Find Help Locally (https://www.cisa.gov/audiences/find-help-locally)
- CISA Cross-sector Cybersecurity Performance Goals (https://www.cisa.gov/cross-sector-cybersecurity-performance-goals)
- NIST Cybersecurity Framework Tools (https://www.nist.gov/cyberframework)

Additional 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)

Appendix E: Acronyms

Acronym	Definition
BYOD	Bring Your Own Device
CIRP	Cyber Incident Response Plan
CISA	Cybersecurity and Infrastructure Security Agency
CPG	Cybersecurity Performance Goals
CSF	Cybersecurity Framework
DHS	U.S. Department of Homeland Security
FBI	Federal Bureau of Investigation
IT	Information Technology
MFA	Multi Factor Authentication
MSP	Managed Service Provider
NHS	National Health Service
NIST	National Institute of Standards and Technology
TLP	Traffic Light Protocol
VoIP	Voice Over Internet Protocol
VSA	Virtual System Administrator
ZTA	Zero Trust Architecture