

**CISA Tabletop Exercise Package Information Technology Sector**

[Enter Organization Name]

<Exercise Date>

Updated June 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc167965173)

[General Information 5](#_Toc167965179)

[Exercise Overview 8](#_Toc167965180)

[Module 1 9](#_Toc167965181)

[Module 2 11](#_Toc167965182)

[Appendix A: Additional Discussion Questions …13](#_Toc167965183)

[Appendix B: Case Studies 16](#_Toc167965184)

[Appendix C: Malicious Activity 18](#_Toc167965185)

[Appendix D: Secure by Design Tactics 19](#_Toc167965186)

[Appendix E: Contacts and Resources 22](#_Toc167965187)

[Appendix F: Acronyms 23](#_Toc167965188)

# 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]](#footnote-2)

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]](#footnote-3) 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](mailto: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: An overview of Secure by Design tactics.
* Appendix E: Additional cybersecurity preparedness and response resources.
* Appendix F: Reference section for acronyms used within this situation manual.

## 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 the threat of supply chain attacks against the IT sector. Your organization pushes a software update to customers. The module ends with the observation of suspicious network activity.
  + **Module 2:** This module continues the scenario with the encryption of your data. Customers report their data was exfiltrated after downloading your software update and subsequently threaten legal action against your organization.
* 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]](#footnote-4)

# 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 | To explore, assess, and enhance plans, procedures, and overall enterprise resilience in response to a significant cyber incident impacting the Information Technology (IT) sector. | |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover | |
| Objectives | 1. Discuss organizational resilience and response to threats targeting the IT sector. 2. Examine plans, policies, and procedures for responding to a cyber incident. 3. Assess internal and external communications processes. | |
| Threat or Hazard | Cyber Attack | |
| Scenario | One of your employees downloads an application infected with malware. A software update your organization pushes to customers is infected with malware as well. Data exfiltration occurs on both your systems and client systems. | |
| Sponsor | Exercise Sponsor | |
| Participating Organizations | Overview of organizations participating in the exercise (e.g., federal, state, local, private sector, etc.). | |
| Points of Contact (POC) | |  |  | | --- | --- | | **Insert Organization POC(s)**  Contact Information | **CISA National Cyber Exercise Program**  [cisa.exercises@cisa.dhs.gov](mailto:cisa.exercises@cisa.dhs.gov)  **IT Sector Risk Management Agency Liaison**  ITSector@cisa.dhs.gov | | |

# Module 1

### Day 1

The Cybersecurity and Infrastructure Security Agency (CISA) releases an alert regarding ongoing malicious activity targeting the Information Technology (IT) Sector.[[4]](#footnote-5) Cyber threat actors targeted multiple software and firmware companies and their customers in a supply chain compromise. Firmware was compromised, potentially leading to multi-stage intrusions against users employing company products. The compromise was linked to state-sponsored cyber actors seeking to compromise U.S.-based software and firmware companies, in what is believed to be a campaign to gain further access to critical infrastructure networks and systems to compromise the core operations and databases of IT sector organizations.[[5]](#footnote-6)

## 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?
   1. What are the possible impacts of an intrusion into your systems?
2. What cybersecurity threat information does your organization receive?
   1. What are your primary sources of information?
   2. How do you determine what information is relevant to your equipment and operations?
   3. What threat information is most useful?
   4. What actions would your organization take in response to a report like the one presented in the scenario?
3. What is the role of cybersecurity in the review and selection of third-party vendor support?
   1. What cybersecurity language (e.g., cybersecurity training and cyber incident notification requirements) is included within third-party vendor contracts?
   2. How do you evaluate the cybersecurity posture of your vendors?
   3. How often are contracts reviewed?

### Day 12

An IT employee supporting the development of your company’s software downloads an application from an official third-party vendor’s site. The application is successfully installed.[[6]](#footnote-7)

1. What are your policies on requesting new software/hardware?
   1. What policies do you have to prevent an end user from downloading unauthorized software?
   2. How do you verify the integrity of third-party software updates before they are implemented?
2. Describe your organization’s cybersecurity training program for employees.
   1. How often are employees required to complete this training?
   2. What additional training is required for employees who have system administrator-level privileges?
   3. What type of training methods or approaches have you found most beneficial?

### Day 20

Your organization publishes an update to your software. Customers are advised to incorporate the update into their software as soon as possible.[[7]](#footnote-8)

1. How does your organization apply Secure by Design principles?[[8]](#footnote-9)
   1. What are your policies and procedures regarding incorporating security into all aspects of software design and development?
   2. Does your organization conduct security assessments and evaluations to ensure security is incorporated into all products?
   3. How are threat models used to identify and mitigate security risks during resource allocation and development?
   4. How does your organization hold product development teams accountable for incorporating security and fortifying products against the most critical and high-impact threats?

### Day 30

An IT employee notices a high volume of network traffic leaving your organization’s servers and going to an unauthorized Internet Protocol (IP) address.[[9]](#footnote-10) Upon investigating, the IP address resolves to a foreign country.

1. How does your organization baseline network activity?
   1. How do you distinguish between normal and abnormal traffic?
   2. What are your next steps when abnormal activity is detected/reported?
   3. What intelligence feeds for indicators of compromise does your organization use?
2. What steps do you take to ensure organizational data is secure from data loss/theft?
   1. What cybersecurity best practices do you leverage before giving access to sensitive business data?

# Module 2

### Day 31 – Morning

Customers who use your software report evidence of data exfiltration. Customers’ internal logs show large file transfers leaving their networks to unauthorized IP addresses. Some customers are also reporting that financial data was modified and bank accounts with a large amount of money have been redirected to offshore accounts. All impacted customers implemented the recently updated software your company published.[[10]](#footnote-11)

## Discussion Questions

1. Discuss your organization’s procedures for declaring a cyber incident.
   1. What escalation criteria is defined in your cyber incident response plan?
2. How sufficient are your organization’s current internal resources for responding to the cyber incidents in this scenario?
   1. What additional resources outside of your organization are necessary for responding to the cyber incident?
   2. What are the processes or procedures for requesting additional resources?
   3. What external partners (e.g., CISA, FBI, vendors) would you contact for assistance?
3. How do you know which of your customers are affected by this incident?
   1. What actions do you take to support incident response for your customers?
   2. What actions are needed to mitigate any reputational damage?

### Day 31 – Afternoon

The team investigating the data exfiltration discovers the impacted data is now encrypted and no longer accessible. Impacted data includes your organization’s core databases, files, and programs, halting your operations. Your software development teams are unable to continue their work, and other teams are unable to troubleshoot customer complaints.

1. Does your organization have backups of important files stored in a location separate from your primary working files/copies?
   1. How long would it take to restore primary files from backups?
   2. How frequently do you test restoration from backups?
   3. How long do you keep copies of archived files backed up?
2. What policies and procedures does your organization use to decide when and how to restore backed-up data?
   1. How does your organization incorporate measures for ensuring the integrity of backup data before restoration?
3. Are you able to continue to provide services to your customers while responding to this incident?
   1. What alternative systems or manual processes are implemented to continue operations if a critical system is unavailable for a significant period?
   2. Who can authorize the use of alternate systems or procedures?
   3. How long can you operate using manual processes or alternate systems when your primary critical systems fail?
   4. What additional staffing requirements are necessary for alternate systems or procedures?

### Day 33

Your customers threaten to sue your organization over the loss of their sensitive data. Reporters contact your organization for comment.

1. What incident-related information are you sharing internally (e.g., with employees, leadership)?
2. What incident-related information are you sharing externally (e.g., with customers, partners)?
   1. How do you respond to the media inquiries?
3. What legal and regulatory notifications are required based on the scenario?
4. When are notifications made?
5. Who is responsible for making the notifications?
6. What is your legal liability if your software update is found to be the source of a cyber incident impacting your customers?
7. How would you work to regain public trust and the trust of your customers following this incident?

### Day 50

Your organization confirms malicious actors gained access and planted the malware in your system via the compromised third-party application your employee downloaded. Once in the network, threat actors moved laterally, using elevated privileges to gain access to software that was under development at the time. Threat actors compromised the software before development was complete. Your organization then unknowingly published a compromised version of your software.

1. When would your organization transition to the recovery and post-incident phases?
   1. How does your organization conduct post-incident reviews?
   2. How are lessons learned/areas for improvement incorporated into process improvement planning (e.g., incident response plans, training, etc.)?
2. How do you verify the integrity of your critical systems following a cyber incident?
   1. How do you assure your customers that future software updates will incorporate Secure by Design principles and security considerations?[[11]](#footnote-12)
   2. What actions do you take to mitigate future vulnerabilities in software development?
3. Based on discussion and lessons learned, what changes will you implement to increase the resilience of your organization?

# 

# 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 paragraph, as well as undesired discussion questions, should be deleted.***

## Cyber Resilience

1. What additional features (e.g., multifactor authentication (MFA), access controls, etc.) can your organization implement to increase organizational resilience and follow Secure by Design principles?
2. How is defense-in-depth incorporated into your organizational system/network security?
   1. Are there any areas where defense-in-depth practices could be strengthened?
3. Discuss how cyber preparedness is integrated with your current all-hazards preparedness efforts.
4. Describe your organization’s patch management and vulnerability management plans.
   1. Does your organization apply Zero Trust Architecture (ZTA)/zero-trust concepts?
   2. Describe your policies on remote access to your organization’s network.
   3. What security protocols (MFA, encryption, etc.) exist on your hardware or software?
5. How often are your cybersecurity plans, policies, and procedures externally reviewed or audited?
   1. What were the most recent results and action items that followed?
6. Discuss your risk management strategy.
7. How is it developed/maintained?
8. What considerations are addressed in your risk management strategy (e.g., extended downtime, impaired functionality, loss of data, etc.)?
9. Describe the relationship between the IT risk management strategy and the enterprise risk management strategy.
10. What are the cybersecurity objectives for your organization?
    1. How do these align with your business objectives?
11. Describe your organization’s review process for your cyber incident response plan (CIRP).
12. How is your CIRP integrated with other incident or emergency response/management plans?
13. How often is the CIRP reviewed?
14. Which individual(s) and department(s) are responsible for reviewing and updating the plan?
15. How are updates to the plan communicated to department or agency employees?
16. How is the integrity of your critical data protected and validated?
17. What external entities have access to your data?
18. How would those entities report a breach of their systems to your office?
19. What essential functions are impacted by the incidents described in the scenario?
20. If primary communications are compromised, how do you provide information to internal and external entities?

## Accounts & Privileges

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

## Incident Identification

1. How are cyber incidents reported within your organization?
2. What would trigger the reporting requirements established by regulation, law, and/or organization policy?
3. What training do employees receive regarding reporting requirements and your cyber incident response plan?
4. What cybersecurity incident escalation criteria are defined in your cyber incident response plan?
5. Who is responsible and what actions would they take based on the scenario?
6. Who should be notified internally and externally according to the plan?
7. When would leadership be notified?
8. Discuss your organization’s intrusion detection capabilities and analytics that alert you to a potential cyber incident.
9. What type of hardware and/or software does your organization use to detect and prevent malicious activity on your systems/network?
10. How often is your organization’s data reviewed?
11. How would you determine whether unauthorized manipulation of data 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?
   1. How would a law enforcement investigation impact containment, eradication, and recovery efforts?
3. What are the processes for contacting critical personnel outside of core hours?
4. How do you proceed if critical personnel are unreachable or unavailable?
5. How would a breach of vendor(s) affect your organization if they have access to your information?
6. What are the notification requirements to your organization for breaches?

## Recovery

* 1. When does your organization determine a cyber incident is resolved?

1. Who makes this decision?
2. What post-incident activities would your organization conduct?
   1. What actions would your organization take if your IT/incident response staff could not confirm the integrity of your systems/data?
3. What is the risk associated with reactivating critical business processes and systems?
4. Describe the process to completely rebuild these systems.
5. 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?
2. What additional training and/or exercise requirements do you require for your incident response staff?
3. How often does your organization exercise its CIRP?
4. Who is involved in the exercises?
5. What external agencies are involved in the exercises?
6. How often do senior staff/leadership participate in cybersecurity exercises?

## Senior Leaders

1. As a leader in your organization, what cybersecurity resilience goals have you set?
2. How do these goals align with organizational objectives?
3. Are there ways the leadership can better support a Secure by Design-oriented organization?
4. Describe your organization’s cybersecurity culture.
5. What cybersecurity training is required for senior leadership?
6. At what point would you activate your organization’s Security Operations Center/EOC?
7. What is your role during a cyber incident?
8. What information do you need to support your decision-making process?
9. What are the gaps in your cybersecurity workforce?
10. 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 department during a cyber incident?
2. What legal documents does your organization require for cyber incidents?

# Appendix B: Case Studies

## 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 million daily users across multiple sectors.[[12]](#footnote-13) 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.[[13]](#footnote-14)

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.[[14]](#footnote-15)

## Attack Against Software Used by MSPs Causes Major Downstream Impacts

A ransomware attack targeted a software provider used by numerous managed service providers (MSPs), causing significant downstream operational impacts in July 2021.[[15]](#footnote-16) 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.[[16]](#footnote-17)

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.[[17]](#footnote-18) 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[[18]](#footnote-19) and eventually obtained the decryption tool from an undisclosed third party to restore the encrypted data of impacted organizations.[[19]](#footnote-20)

## Impacts of Trojanized Supply Chain Attack Felt Worldwide

In June of 2017, Russian hackers launched a new version of Petya ransomware, named NotPetya, that acted more like destructive malware than ransomware. NotPetya was placed within an update to an accounting software widely used by Ukrainian businesses and quickly spread worldwide. The malware severely impacted operations across sectors, creating major shipping, banking, and manufacturing disruptions in multiple countries, including the United States.[[20]](#footnote-21) NotPetya propagated rapidly, required no user interaction to run, and autonomously spread to every networked system by leveraging known vulnerabilities in older versions of Windows operating systems. The malware stole stored user credentials and leveraged them to gain further network access.[[21]](#footnote-22) EternalBlue, a key vulnerability NotPetya used to spread, was identified and patched during the WannaCry attack in the months prior. Leaving the EternalBlue vulnerability unpatched exposed victims to exploitation.

# Appendix C: Malicious Activity

## Software Supply Chain Compromises

A software supply chain compromises 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>)

# Appendix D: Secure by Design Tactics

Memory Safe Programming Languages

The use of memory safe program languages is a key principle of Secure by Design. Common memory safe programming languages include C#, Go, Java, Ruby, Rust, and more. Memory safety is critical because many vulnerabilities stem from how a program manages memory. In non-safe languages, a common vulnerability is a buffer overflow, where data outside of the bounds of the program itself is accessed. Malicious actors can abuse this vulnerability to take control of a system. Shorter-term mitigation techniques such as C/C++ language improvements, hardware mitigations, address space layout randomization, control-flow integrity, and fuzzers/sanitizers are lower-cost approaches that improve the security posture of software end-users.

Hardware Security

Architectural features that enable fine-grained memory production should be incorporated in the software development process. These features include the Trusted Platform Module, which stores certificates, passwords, and credentials away from malicious actors’ reach, the Capability Hardware Enhanced RISC Instructions that can extend conventional hardware Instruction-Set Architectures, and Hardware Security Modules, which allow for more secure cryptographic key management.

Secure Software Components

Secure software components such as software libraries, modules, middleware, and frameworks should be acquired from verified commercial, open source, and other trusted third-party developers to ensure the security of consumer software products.

Web Template Frameworks

Web template frameworks are tools and software libraries that facilitate easy web development and contain intrinsic security against intrusion techniques such as cross-site scripting. Web frameworks are widely available, so choosing one that includes input validation, encryption, and other defense methods is a simple way to boost the security of a web project. Aside from protection against cross-site scripting, secure web frameworks also include security against structured query language (SQL) injection and cross-site request forgery.

Parameterized Queries

Parameterizing queries defends against SQL injection techniques. Not using parameterization allows users to input strings into fields that are processed by the SQL server as commands, allowing a level of access to data stored in the database that should not be available, and the capability to modify the data or execute malicious commands.

Static and Dynamic Application Security Testing

Use static and dynamic application security testing tools such as code analyzers and application behavior tools detect error-prone practices in your software such as improper management of memory and error prone database query construction. These tools should be integrated into the development process along with other testing methods such as unit and integration testing, to ensure your software is prepared for deployment.

Code Review

Code review is the core quality assurance process for software developers. Code review should include analysis by both other software developers and by automated programs. The more widespread the use of the code will be, the more reviewers should participate in the process. Code reviews are a key part of application security, helping to detect security gaps and vulnerabilities before software goes live. The more often code review occurs within an organization, the more attuned developers are to discovering issues and improving their own development strategies and processes as well.

Software Bill of Materials

A Software Bill of Materials (SBOM) is a list of the open source and third-party components used in a piece of software. The SBOM includes details such as the version of the components, aiding security personnel in identifying compromised software when a vulnerability is discovered in these underlying components. This is critical in a supply chain compromise, allowing identification of software at risk from the incident.

Vulnerability Disclosure Programs

Vulnerability disclosure programs provide a secure pathway for security researchers to report vulnerabilities within software safely and quickly expedite the remediation process. These programs should include pipelines that carry issues from their initial reporting through to remediation.

Common Vulnerabilities and Exposure (CVE) Completeness

Ensure published CVEs include root cause or common weakness enumeration to enable industry-wide analysis of software security design flaws. The more detailed a CVE is, the greater the ability for the industry to use the lessons learned to prevent future vulnerabilities.

Defense-in-Depth

Defense-in-depth ensures no single security layer stands alone in preventing compromise. Ensuring user privileges are narrowly provisioned and access control lists are employed to reduce the potential impact of a compromised account is an example of this method. Sound defense-in-depth application includes using detection methodologies to observe a compromise and immediately engaging sandboxing techniques to quarantine a vulnerability to defend against potential exploitation.

Satisfy Cybersecurity Performance Goals (CPGs)

CISA’s CPGs provide the baseline security measures organizations should implement. Fulfilling the CPGs in the software development process supports a Secure by Design framework.

### Additional Resources

* CISA Secure by Design (<https://www.cisa.gov/securebydesign>)
* CISA Software Bill of Materials (<https://www.cisa.gov/sbom>)
* CISA Stakeholder-Specific Vulnerability Categorization Methodology to Prioritize Vulnerabilities (<https://www.cisa.gov/news-events/alerts/2022/11/10/cisa-releases-ssvc-methodology-prioritize-vulnerabilities>)
* NIST Computer Security Resource Center – Secure Software Development Framework ([https://csrc.nist.gov/pubs/sp/800/218/final](https://urldefense.us/v3/__https:/csrc.nist.gov/pubs/sp/800/218/final__;!!BClRuOV5cvtbuNI!A-ma1BY4XscABOWHzv7Ey7_SKZBnOVYijzA8KisluVEpN-P6Vcup8Agt-Lu1bJGsJUdwGWed3vuUVWoVmjxrS9-3Drw-OD1PnJI$))
* National Security Agency – Software Memory Safety (<https://media.defense.gov/2022/Nov/10/2003112742/-1/1/0/CSI_SOFTWARE_MEMORY_SAFETY.PDF>)
* University of Cambridge – Capability Hardware Enhanced RISC Instructions (<https://www.cl.cam.ac.uk/research/security/ctsrd/cheri/>)

# Appendix E: Contacts and Resources

Federal Government Contacts

* CISA (contact: [central@cisa.gov](mailto: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 Offices (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](http://www.ic3.gov/))
* National Cyber Investigative Joint Task Force (NCIJTF) CyWatch 24/7 Command Center (contact: [cywatch@ic.fbi.gov](mailto:cywatch@ic.fbi.gov); 855-292-3937)

Information Technology Sector Resources

* CISA IT Sector (<https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors/information-technology-sector>)
* CISA Enduring Security Framework (<https://edit.cisa.gov/resources-tools/groups/enduring-security-framework-esf>)

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>](https://www.nist.gov/cyberframework))

State Level Resources

* Multi-State Information Sharing and Analysis Center (MS-ISAC) (contact: [info@msisac.org](mailto:info@msisac.org); 518-266-3460)
* DHS Fusion Centers (<https://www.dhs.gov/state-and-major-urban-area-fusion-centers>)

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](http://www.certifiedisao.org/); contact: [operations@certifiedisao.org](mailto:operations@certifiedisao.org))
* Information Technology ISAC (<https://www.it-isac.org>)
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

# Appendix F: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BYOD | Bring Your Own Device |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| CPG | Cybersecurity Performance Goals |
| C-SCRM | Cybersecurity Supply Chain Risk Management |
| CSF | Cybersecurity Function |
| CTEP | CISA Tabletop Exercise Package |
| CVE | Common Vulnerabilities and Exposures |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| IOC | Indicators of Compromise |
| IP | Internet Protocol |
| IT | Information Technology |
| MFA | Multi Factor Authentication |
| MSP | Managed Service Provider |
| NCEP | National Cyber Exercise Program |
| NIST | National Institute of Standards and Technology |
| POC | Point of Contact |
| SBOM | Software Bill of Materials |
| SQL | Structured Query Language |
| TLP | Traffic Light Protocol |
| VoIP | Voice over Internet Protocol |
| ZTA | Zero Trust Architecture |

1. “Computer Security Resource Center Glossary: Cyber Resilience,” National Institute of Standards and Technology, accessed August 2, 2023, <https://csrc.nist.gov/glossary/term/cyber_resiliency>. [↑](#footnote-ref-2)
2. “Homeland Security Exercise and Evaluation Program,” FEMA, February 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-3)
3. FEMA, “Homeland Security Exercise and Evaluation Program,” January 2020, <https://www.fema.gov/emergency-managers/national-preparedness/exercises/hseep>. [↑](#footnote-ref-4)
4. CISA “Cybersecurity Alerts and Advisories,” <https://www.cisa.gov/news-events/cybersecurity-advisories> [↑](#footnote-ref-5)
5. CISA CPG Checklist, “3.A – Detecting Relevant Threats & TTPs,” [<https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist>](https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist) [↑](#footnote-ref-6)
6. CISA CPG Checklist, “2.I – Basic Cybersecurity Training,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-7)
7. CISA CPG, “1.E – Mitigating Known Vulnerabilities,” <https://www.cisa.gov/resources-tools/resources/cisa-cpg-checklist> [↑](#footnote-ref-8)
8. CISA, “Secure by Design,” <https://www.cisa.gov/securebydesign> [↑](#footnote-ref-9)
9. NIST CSF 2.0, “DE.CM: Continuous Monitoring,” <https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters> [↑](#footnote-ref-10)
10. NIST CSF 2.0, “Adverse Event Analysis (DE.AE),” <https://csrc.nist.gov/Projects/Cybersecurity-Framework/Filters#/csf/filters> [↑](#footnote-ref-11)
11. CISA, “Secure by Design,” <https://www.cisa.gov/securebydesign> [↑](#footnote-ref-12)
12. 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/>. [↑](#footnote-ref-13)
13. 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>. [↑](#footnote-ref-14)
14. 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>. [↑](#footnote-ref-15)
15. 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>. [↑](#footnote-ref-16)
16. 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>. [↑](#footnote-ref-17)
17. 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>. [↑](#footnote-ref-18)
18. Joe Tidy, “Swedish Coop supermarkets shut due to US ransomware cyber-attack,” *BBC,* July 3, 2021, <https://www.bbc.com/news/technology-57707530>. [↑](#footnote-ref-19)
19. Kaseya, “Important Notice August 4th, 2021,” <https://helpdesk.kaseya.com/hc/en-gb/articles/4403440684689-Important-Notice-July-3rd-2021>. [↑](#footnote-ref-20)
20. The Federal Reserve Bank of New York, “Pirates Without Borders: The Propagation of Cyberattacks through Firms’ Supply Chains,” July 2021, <https://www.newyorkfed.org/research/staff_reports/sr937>. [↑](#footnote-ref-21)
21. CISA, “Petya Ransomware,” February 15, 2018, <https://www.cisa.gov/news-events/alerts/2017/07/01/petya-ransomware>. [↑](#footnote-ref-22)