

**CISA Tabletop Exercise Package For Executives/Senior Leadership**

[Enter Organization Name]

<Exercise Date>

Updated August 2024

Cybersecurity and Infrastructure Security Agency

Table of Contents

[Handling Instructions 3](#_Toc169522950)

[General Information 5](#_Toc169522956)

[Exercise Overview 8](#_Toc169522957)

[General Discussion Questions 9](#_Toc169522958)

[Vignette 1: Whaling/Ransomware 10](#_Toc169522959)

[Vignette 2: Insider Threat 11](#_Toc169522960)

[Appendix A: Case Studies 13](#_Toc169522961)

[Appendix B: Malicious Activity 14](#_Toc169522962)

[Appendix C: Contacts and Resources 16](#_Toc169522963)

[Appendix D: Acronyms 17](#_Toc169522964)

# 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 (TTX). A TTX 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

Vignettes 1 and 2 contain the scenario 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: Case studies that provide real-world examples of the threats presented in this scenario.
* Appendix B: An explanation of the threats presented in this scenario.
* Appendix C: Additional cybersecurity preparedness and response resources.
* Appendix D: 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 senior-level leadership, the Chief Information Security Officer/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 specific 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 will be a facilitated discussion-based TTX. Each vignette in this Situation Manual is designed to be conducted as a stand-alone TTX or used in succession for a longer TTX. **Vignettes 1 and 2 are each an isolated series of events that do not relate or apply to the other.** Discussion topics should differ between each vignette. Players will participate in the following:

* Stand-alone scenario vignettes:
  + Vignette 1: A suspicious whaling email leads to a ransomware attack.
  + Vignette 2: A disgruntled former employee steals critical files/data from your organization/jurisdiction.
* Hotwash
* ***Structure Note:*** *Scenario details and discussion questions included in each Vignette may be modified as desired to achieve your specific goals.*

## 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. – 10:30 a.m.)  Exercise Location |
| Purpose | Assess the cyber resilience of <organization/jurisdiction> and the ability to respond to a cyber incident. |
| National Institute of Standards and Technology Cybersecurity Framework Functions | Govern, Identify, Protect, Detect, Respond, Recover |
| Objectives | 1. Identify ways to enhance the cybersecurity resilience of your organization. 2. Improve the decision-making process of senior leadership during a cyber incident. 3. Examine the roles and responsibilities of senior leadership in response to a cyber incident. 4. Discuss the reputational risks and impacts on business operations in the event of a cyber incident. |
| Threat or Hazard | Cyber Incident |
| Scenario | Vignette 1: A threat actor targets a senior executive through a whaling email as an entry point into networks/systems, then installs ransomware on the network.  Vignette 2: A disgruntled former employee uses administrator-level access to systems to steal and delete critical organizational information/data. |
| 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](mailto:cisa.exercises@cisa.dhs.gov) | |

# General Discussion Questions

The general discussion questions below are designed to be used with both vignettes. They may be asked before or after reviewing the vignette scenario. The discussion questions address your organization’s cybersecurity program and organizational risk management.

1. What are the greatest cyber threats to your organization?
2. Describe your cybersecurity culture.[[4]](#footnote-5)
   1. How do you articulate the importance of a strong cybersecurity culture and resiliency to your organization?[[5]](#footnote-6)
   2. How do you enforce a strong cybersecurity culture?
3. What are the cybersecurity objectives for your organization?
   1. How do these align with your business objectives?
4. Describe the relationship between senior leadership, business/application management, and security management (e.g., security steering committee).
   1. What is your overall cybersecurity strategy/plan?
   2. In what ways is your cybersecurity strategy/plan supported and advocated for by senior leadership?
   3. How frequently does the security steering committee communicate with senior leadership?
5. Discuss senior leadership’s role in the management of the cybersecurity program.
   1. How does senior leadership consider cost-benefit and business impact analyses to determine appropriate risk mitigation, continuity, and cybersecurity measures?
   2. How does senior leadership oversee the lifecycle management of the cybersecurity program?
   3. How is senior leadership involved in the development of cybersecurity policies?
   4. How often is senior leadership briefed on the state of your cybersecurity program?
6. Are currently allocated funding and/or resources devoted to cybersecurity sufficient?
   1. What additional resources, if any, might your organization require to respond to and recover from a cyber incident?
7. How does your organization use artificial intelligence (AI)?
   1. What cybersecurity vulnerabilities stem from the use of AI technology?
8. Describe your organization’s cybersecurity training for senior leadership and those with elevated administrative privileges.

# Vignette 1: Whaling/Ransomware

## Scenario

A senior finance employee receives what appears to be an email from another senior-level employee urgently requesting they review a shared document.[[6]](#footnote-7) The following month, employees begin reporting to <HR/Finance/Payroll> that their paychecks were not deposited into their bank accounts. <HR/Finance/Payroll> investigates and finds your payroll system is not working properly.

The next day, all employees are locked out of their computers via ransomware. A ransom note is displayed on employee computers, threatening to sell <employee and/or customer personally Identifiable information (PII)> on the dark web if the ransom of <$XXX,XXX> is not paid. A small amount of <employee and/or customer> bank account information is posted on the dark web as proof of the threat.

### Discussion Questions

1. What is your role during cyber incident response?[[7]](#footnote-8)
   1. At what point would you be notified and/or involved in this scenario?
2. When would you activate your Cyber Incident Response Plan (CIRP) and/or Business Continuity Plan (BCP)/Continuity of Operations (COOP) Plan?
   1. Who is authorized to activate the CIRP/COOP/BCP?
3. How would your organization continue essential functions/operations if a business-critical IT system is unavailable for a significant period of time?
4. Discuss your decision-making process for responding to ransomware.
   1. Does your organization have a ransomware policy?
   2. Explain how your response partners, such as your cyber insurance provider or third-party vendors, are involved in your procedures.
5. If you have cyber insurance, what is their role in incident response?
   1. What does your cyber insurance policy cover?
6. What regulatory and/or compliance requirements must be addressed by senior leadership?
   1. When and how would legal counsel be involved?

# Vignette 2: Insider Threat

## Scenario

Your IT department determines that a known exploited vulnerability on the network is not currently a priority for patching/mitigation.[[8]](#footnote-9) The next day, a disgruntled senior-level IT employee is terminated. Before departing, the employee angrily accuses your organization of wrongful termination.

One month later, several employees contact the help desk reporting they cannot access information on network shared drives. IT investigates and discovers sensitive files <including intellectual property/protected files> appear to have been removed.[[9]](#footnote-10) Upon further investigation, an administrator account accessed file servers throughout the network and exfiltrated data to an external IP address. This account belonged to the terminated employee.

A post goes viral on social media in which an anonymous hacker claims responsibility for the breach and theft of critical information, including sensitive employee information, from your organization and that of your <customers/constituents/partners/shareholders>.

<Customers/constituents/partners/shareholders> are requesting information about the breach. Media outlets are also requesting comments and interviews.

### Discussion Questions

1. How does your organization mitigate insider threats?
   1. Does your organization have an insider threat management program?
   2. What type of training do senior leaders at your organization receive on identifying a potential insider threat?
2. In this scenario, how are you communicating with and what is your message to:
   1. Employees/customers?
   2. Management?
   3. Shareholders/constituents?
   4. Partners/contractors/vendors?
   5. Media?
3. What are the reputational impacts of this incident?[[10]](#footnote-11)
   1. How will you manage these impacts?
   2. How would you address concerns and mistrust from <employees, partners, shareholders, vendors, customers, constituents>?
   3. Is there funding available to pay for credit monitoring for impacted individuals?
4. Discuss how lessons learned from incidents are briefed to you.[[11]](#footnote-12)
   1. How are lessons learned incorporated into new cybersecurity policies?
   2. Who leads policy development?
   3. Who is part of the approval process?

# Appendix A: Case Studies

## Whaling Attack Devastates Hedge Fund

In late 2020, an Australian hedge fund was forced to close after falling victim to a whaling attack. The company inadvertently paid three fraudulent invoices totaling $8 million. This led to one of their largest investors pulling out of a $16 million investment deal, consequently forcing the hedge fund to permanently end operations.

Investigators determined one of the hedge fund’s co-founders clicked a fake Zoom meeting link, thereby releasing malware onto their systems. The threat actor managed to infiltrate the hedge fund’s email system and took over one of the co-founders’ email accounts. From there, a series of fraudulent invoices were sent to a trustee and an administrator, who then paid the invoices, believing they were legitimate. The money went directly to the threat actor and was not recovered.[[12]](#footnote-13)

## Sensitive Client Information Stolen by Insider

The parent company of a mobile payment application (app) reported a data breach of the app’s client information in early December 2021. A former employee accessed and downloaded sensitive customer financial data after leaving the company. The stolen data included customer names, brokerage account numbers, brokerage portfolio values and holdings, and stock trading information.[[13]](#footnote-14) The payment app notified law enforcement and conducted a forensic investigation to address the issue, emphasizing that company policy states employees’ access is revoked upon leaving the company. A total of 8.2 million current and former clients were notified of the incident.[[14]](#footnote-15)

Inside Hacker Accesses Customer Credentials and Applications

A software engineer for the cloud hosting company contracted by a major financial company to provide cloud based services was accused of infiltrating a company server and obtaining access to 140,000 Social Security numbers, one million Canadian Social Insurance numbers, and 80,000 bank account numbers, along with customers’ personal financial information. The software engineer exploited a misconfigured web firewall to gain entry.[[15]](#footnote-16)

The software engineer did not attempt to remain anonymous; they posted information on social media, posted the stolen data on GitHub using their full name, and shared their hacking method with coworkers via Slack chat. An individual discovered the information on GitHub and alerted the financial company. The incident resulted in a cost of $150 million cost for the company.

# Appendix B: Malicious Activity

## Data Loss and Data Theft

Data theft and malicious data loss is a type of cybercrime where criminals gain access to sensitive and private information that is not meant to be shared publicly. This data can be as simple as names and addresses and escalate to operational script/code and proprietary research. Once the information has been ascertained the data is often copied and used to commit the crime of identity theft or as a way to exfiltrate money from victims. The economic and reputational impacts of data loss/theft on individuals and organizations can be significant. Losses can include damage to productivity, continuity of operations disruption, financial cost from investigation and recovery, financial costs due to lawsuits from customers, employees, or regulatory penalties, and overall reputational damage. To mitigate data theft/loss it is necessary to know what personal and sensitive information is on your network or systems, know who has access to it, encrypt sensitive information, implement firewalls, apply network segmentation, and ensure your CIRP and Communications Plan include response and notification procedures for data breach incidents.

### Additional Resources

* Protecting Sensitive and Personal Information (<https://www.cisa.gov/resources-tools/resources/protecting-sensitive-and-personal-information>)
* Cybersecurity and Physical Security Convergence Action Guide (<https://www.cisa.gov/resources-tools/resources/cybersecurity-and-physical-security-convergence-action-guide>)

## 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>)

## Insider Threat

An insider threat is the potential for someone with authorized access or understanding of an organization to harm the organization. This cyber threat includes theft, espionage, violence, and sabotage of anything related to technology, virtual reality, computers, devices, or the internet. Unintentional threats are the non-malicious (accidental or inadvertent) exposure of an organization’s IT infrastructure, systems, and data that causes unintended harm to an organization. Intentional threats are malicious actions performed by insiders with malintent who use technical means to disrupt or halt an organization’s business operations, identify IT weaknesses, gain protected information, or otherwise further an attack plan via access to IT systems. This action can involve changing data or inserting malware or other pieces of offensive software to disrupt systems and networks. Successful mitigation of insider threats and insider threat programs requires the detection and identification of observable, concerning behaviors or activities and the subsequent implementation of measures to manage the risk of potential harmful actions.

### Additional Resources

* CISA Insider Threat Mitigation Guide (<https://www.cisa.gov/resources-tools/resources/insider-threat-mitigation-guide>)
* Insider Threat Mitigation (<https://www.cisa.gov/topics/physical-security/insider-threat-mitigation>)

## 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, whaling, 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 C: Contacts and Resources

Federal Government Resources

* CISA (contact: [central@cisa.gov](mailto:central@cisa.gov), <https://www.cisa.gov>)
* Federal Bureau of Investigation (FBI)
* Field Office Cyber Task Forces (contact: <https://www.fbi.gov/contact-us/field-offices>)
* Internet Crime Complain Center (IC3) (contact: [http://www.ic3.gov](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)
* 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>)

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))
* National Council of ISACs ([https://www.nationalisacs.org](https://www.nationalisacs.org/))

# Appendix D: Acronyms

|  |  |
| --- | --- |
| Acronym | Definition |
| BCP | Business Continuity Plan |
| BIA | Business Impact Analysis |
| CIRP | Cyber Incident Response Plan |
| CISA | Cybersecurity and Infrastructure Security Agency |
| COOP | Continuity of Operations Plan |
| CPG | Cybersecurity Performance Goals |
| DHS | U.S. Department of Homeland Security |
| FBI | Federal Bureau of Investigation |
| HR | Human Resources |
| IT | Information Technology |
| NIST | National Institute of Standards and Technology |
| PII | Personally Identifiable Information |
| TLP | Traffic Light Protocol |

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>. [↑](#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. NIST Cybersecurity Framework v2.0 (CSF 2.0) via NIST’s CPRT, “GV: Governance,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV>. [↑](#footnote-ref-5)
5. CSF 2.0 via CPRT, “GV.PO: Policy – Organizational cybersecurity policy is established, communicated, and enforced,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=GV.PO>. [↑](#footnote-ref-6)
6. Cybersecurity Framework, v2.0 (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>. [↑](#footnote-ref-7)
7. 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?element=ID.IM-04>. [↑](#footnote-ref-8)
8. CSF 2.0 via CPRT, “ID.RA-06: Risk responses are chosen, prioritized, planned, tracked, and communicated,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=ID.RA-06>. [↑](#footnote-ref-9)
9. 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>. [↑](#footnote-ref-10)
10. CSF 2.0 via CPRT, “RC.CO-04: Public updates on incident recovery are shared using approved methods and messaging,” <https://csrc.nist.gov/projects/cprt/catalog#/cprt/framework/version/CSF_2_0_0/home?element=RC.CO-04>. [↑](#footnote-ref-11)
11. 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>. [↑](#footnote-ref-12)
12. “Levitas Capital Closing After Fake Zoom Invite Sink $16m Super Fund Investment,” *News.com.au,* (November 23, 2020, <https://www.news.com.au/technology/online/security/levitas-capital-closing-after-fake-zoom-invite-sinks-16m-super-fund-investment/news-story/110750489020507558921a95cbe2c980>. [↑](#footnote-ref-13)
13. S. Fadilpašić, “Cash App alerts 8 million customers to data breach,” *Tech Radar,* April 6, 2022, <https://www.techradar.com/news/cash-app-alerts-8-million-customers-to-data-breach>. [↑](#footnote-ref-14)
14. S. Wadhwani, “Block’s Cash App Suffers Serious Insider Theft, Customers’ Brokerage Accounts Compromised,” *Spiceworks,* April 6, 2022, <https://www.spiceworks.com/it-security/data-security/news/block-cash-app-data-insider-theft/>. [↑](#footnote-ref-15)
15. # Rob McLean, ” A hacker gained access to 100 million Capital One credit card applications and accounts,” *CNN,* July, 30 2019,

    <https://www.cnn.com/2019/07/29/business/capital-one-data-breach/index.html>. [↑](#footnote-ref-16)