

SHIELDS UP

A BRIEF OVERVIEW OF RECOMMENDED ACTIONS AND RESOURCES FOR IMPROVING NEAR-TERM CYBER RESILIENCE



Ernesto Ballesteros, JD, MS, CISSP, CISA, Security+

Cybersecurity State Coordinator of Texas

CISA Region 6

Objectives

1. Inform the audience of CISA's mission, vision, and no-cost cybersecurity resources
2. Inform the audience of foundational cybersecurity concepts
3. Inform the audience of near-term cybersecurity practices that organizations should consider to adopt a heightened cybersecurity posture
4. Inform the audience of how they can engage CISA and explore opportunities to partner on cybersecurity matters



CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

CISA partners with industry and
government to understand and
manage risk to our Nation's
critical infrastructure.



OVERALL GOALS

GOAL 1

DEFEND TODAY

Defend against urgent
threats and hazards

seconds | days | weeks

GOAL 2

SECURE TOMORROW

Strengthen critical
infrastructure and
address long-term risks

months | years | decades

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future



PARTNERSHIP
DEVELOPMENT



INFORMATION AND
DATA SHARING



CAPACITY BUILDING



INCIDENT
MANAGEMENT
& RESPONSE



RISK ASSESSMENT
AND ANALYSIS



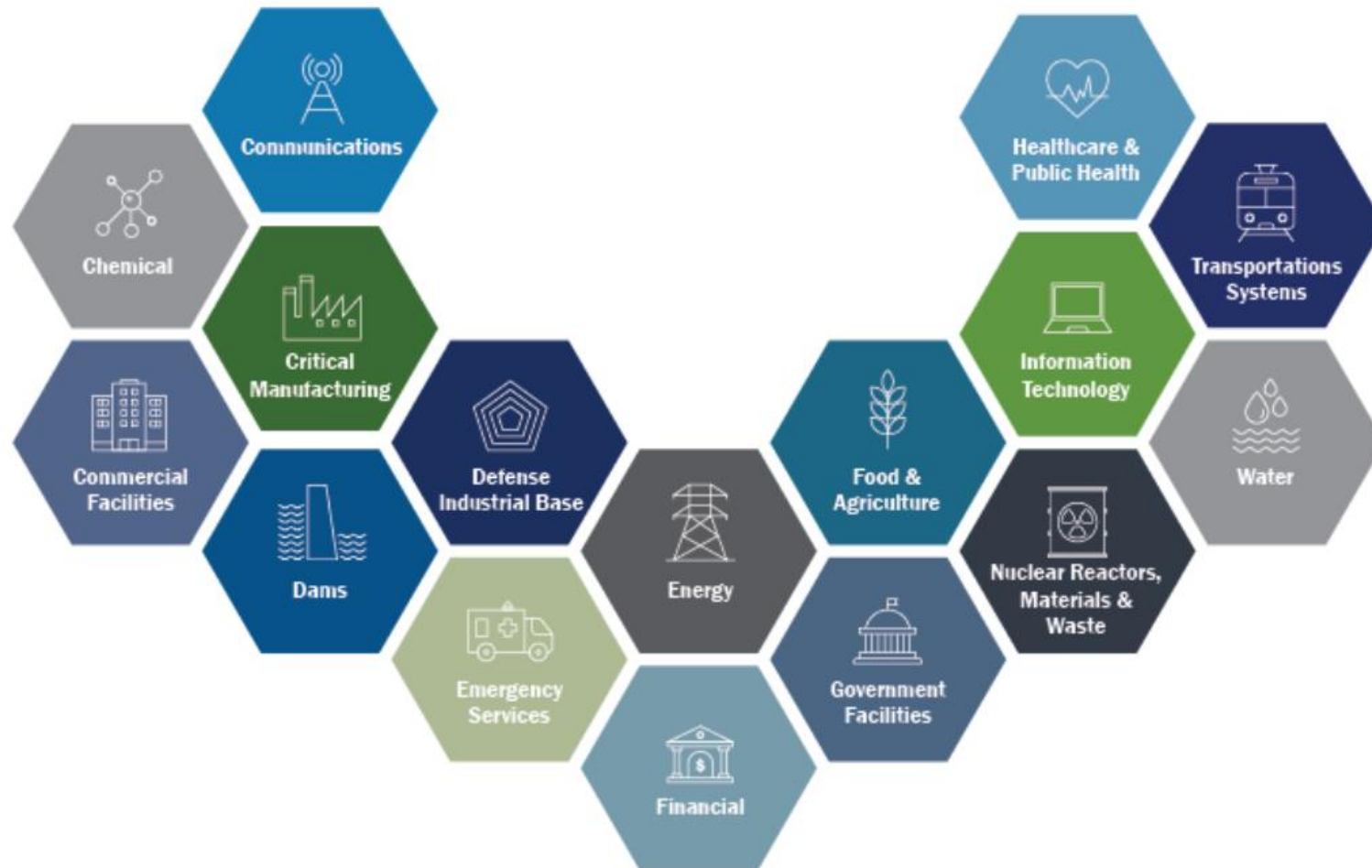
NETWORK DEFENSE



EMERGENCY
COMMUNICATIONS

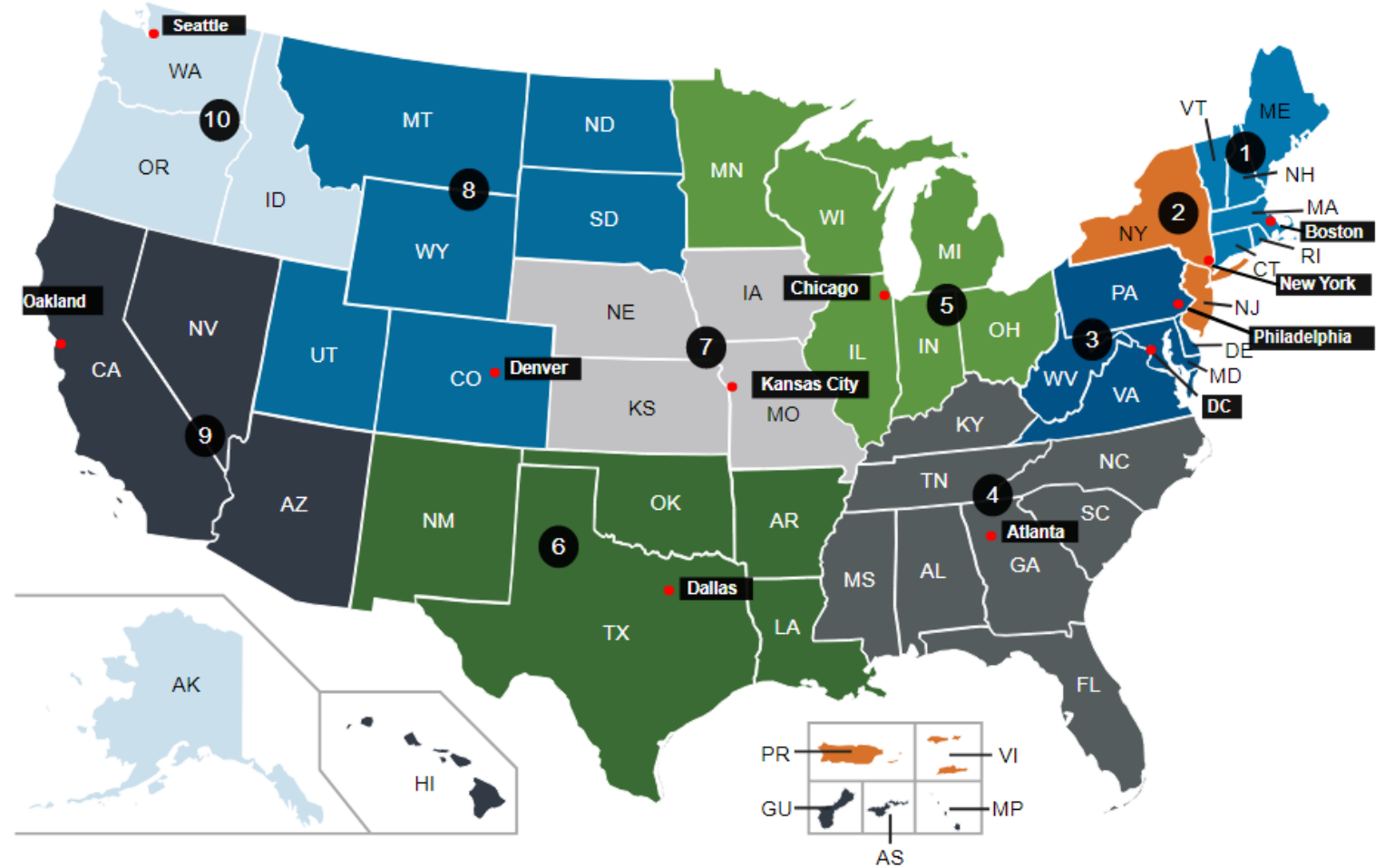
Critical Infrastructure Sectors

CISA assists the public and private sectors to secure their networks and focuses on organizations in the following [16 critical infrastructure sectors](#).



CISA Regions

Region	Location
1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Dallas, TX
7	Kansas City, MO
8	Denver, CO
9	Oakland, CA
10	Seattle, WA



<https://www.cisa.gov/cisa-regions>

Cybersecurity State Coordinator (CSC)

The role of the Cybersecurity State Coordinator (CSC) is to build strategic public and private sector relationships in Texas to facilitate the development and maintenance of secure and resilient infrastructure, pursuant to [6 United States Code, Section 665\(c\) \(2021\)](#).

- Build strategic public and private sector relationships;
- Serve as the Federal cybersecurity risk advisor;
- Facilitate the sharing of cyber threat information;
- Raise awareness of cyber resources from the Federal Government to non-Federal entities;
- Support training, exercises, and planning for continuity of operations from cyber incidents;
- Serve as a principal point of contact for non-Federal entities to engage the Federal Government on preparing, managing, and responding to cyber incidents;
- Assist State, local, Tribal, and territorial governments in development of State cyber plans;
- Coordinate with appropriate officials within the Agency (CISA).



Cybersecurity Advisors (CSAs)

To provide direct coordination, outreach, and regional support in order to protect cyber components essential to the sustainability, preparedness, and protection of the Nation's Critical Infrastructure and Key Resources (CIKR) and State, Local, Tribal, and Territorial (SLTT) governments.

- **Assess:** Evaluate critical infrastructure cyber risk.
- **Promote:** Encourage best practices and risk mitigation strategies.
- **Build:** Initiate, develop capacity, and support cyber communities-of-interest and working groups.
- **Educate:** Inform and raise awareness.
- **Listen:** Collect stakeholder requirements.
- **Coordinate:** Bring together incident support and lessons learned.



No-Cost Cyber Resources and Assessments

Regional Cybersecurity Resources:

- Cybersecurity Assessments (*Performed by Cybersecurity Advisors*)
 - Introductory Level:
 - Ransomware Readiness Assessment (RRA)
 - Cybersecurity Performance Goals Assessment (CPG)
 - Intermediate Level:
 - Cyber Infrastructure Survey (CIS)
 - Advanced Level:
 - Cyber Resilience Review (CRR)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
- Cybersecurity Exercises and Workshops (*Performed by Cybersecurity Advisors*)
 - Cyber Resilience Workshop (CRW)
 - Incident Management Workshop (IMW)
 - Vulnerability Management Workshop (VMW)
 - Intro to Digital Forensics Workshop (DFW)
 - Facilitated Cyber Exercise (FCE)

National/Automated Cybersecurity Resources:

- Vulnerability Scanning Service (CyHy)



SHIELDS UP



Today's Risk Landscape

America remains at risk
from a variety of threats:



INSIDER THREAT



ACTS OF TERRORISM



CYBER ATTACKS



EXTREME WEATHER



PANDEMICS



ACCIDENTS OR TECHNICAL FAILURES

What is Information Security?

Definition: Information Security

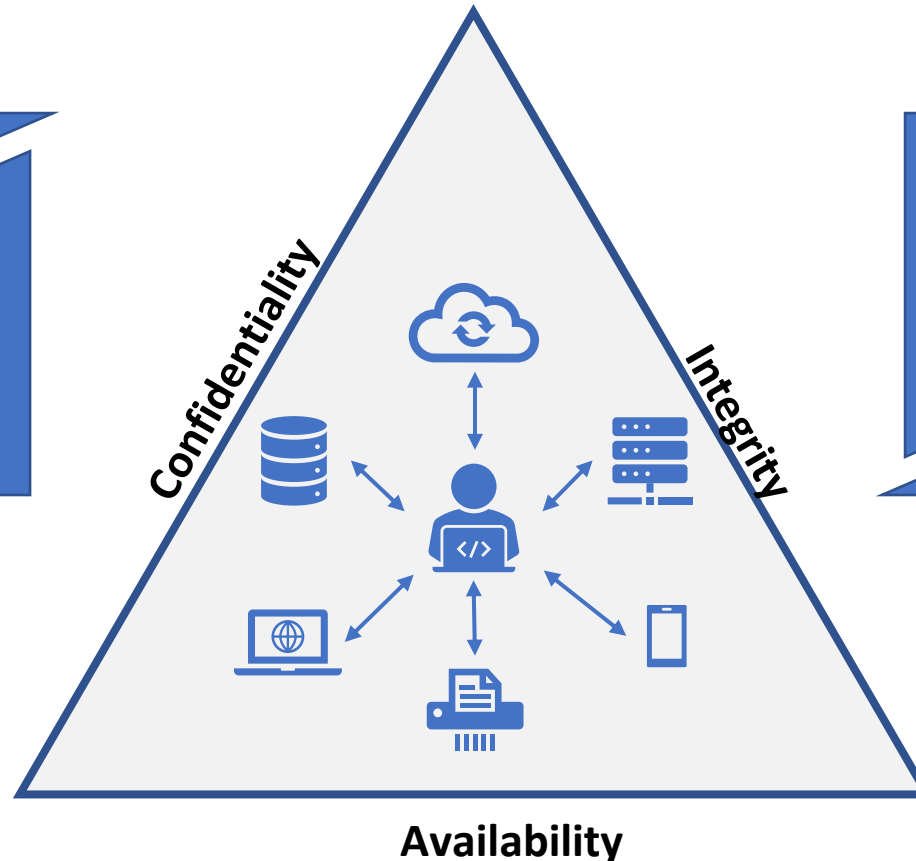
According to NIST, **Information Security** is “[t]he protection of information and information systems against unauthorized access, use, disclosure, modification, or destruction in order to provide confidentiality, integrity, and availability.”

Source: [NIST SP 800-171 Rev. 1](#)



Information refers to “[a]ny communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual.”

Source: [NIST SP 800-171 Rev. 1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#)



Information System refers to “[a] discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.”

Source: [NIST SP 800-53 Rev. 4 Security and Privacy Controls for Federal Information Systems and Organization](#)



Core Objectives of Information Security

C

Prevent unauthorized access and use of information resources

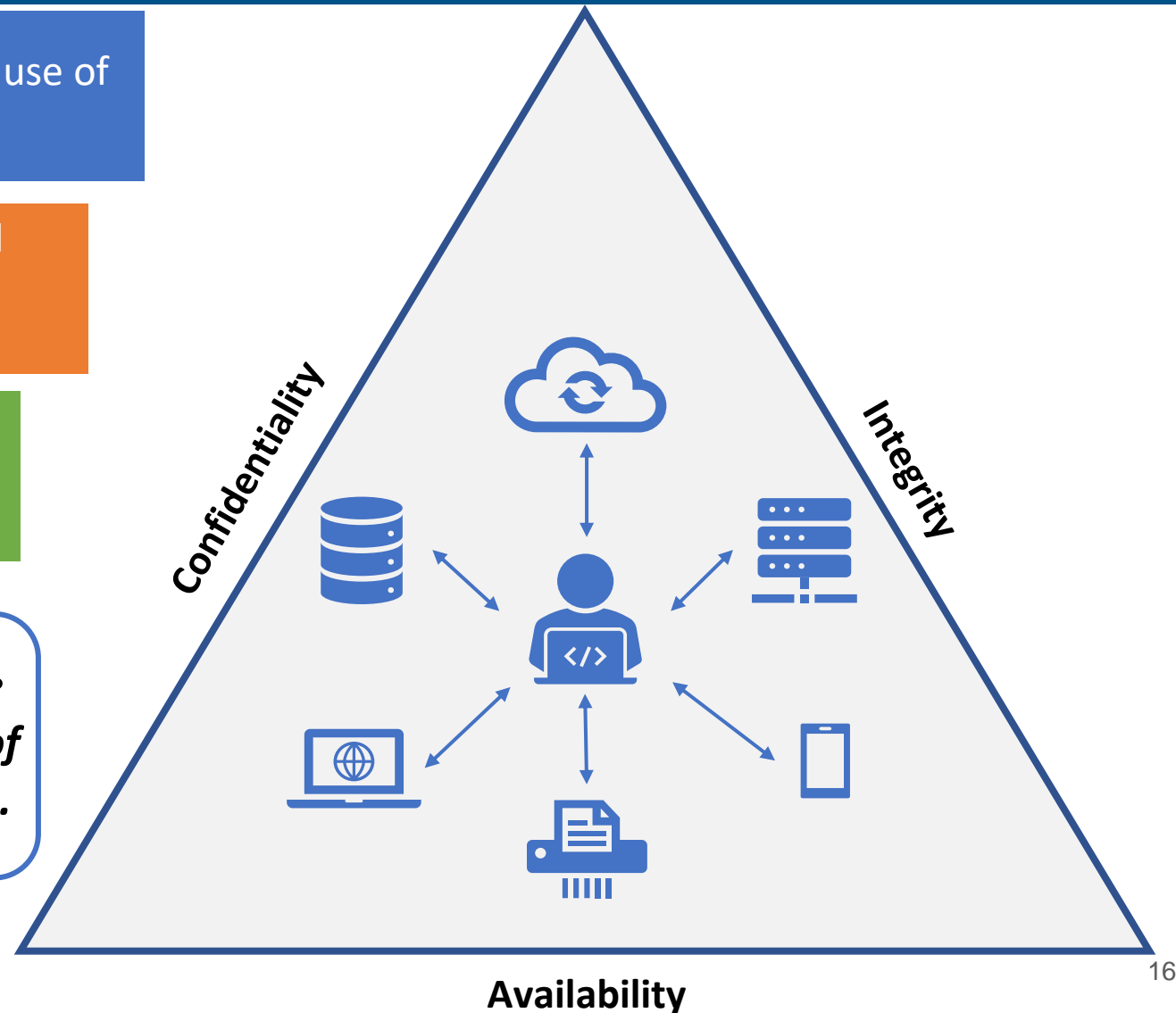
I

Prevent unauthorized change and ensure reliability of information resources

A

Ensure timely availability of information resources

Users must exercise due care to ensure the confidentiality, integrity, and availability of the information resources under their care.

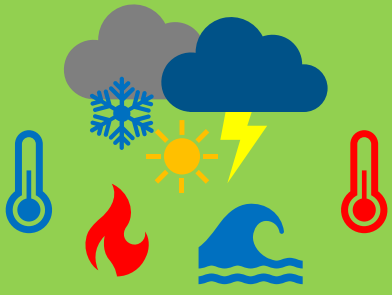


Threats

THREATS

Nature-Based

Threats that naturally occur, such as fires, floods, or hurricanes.

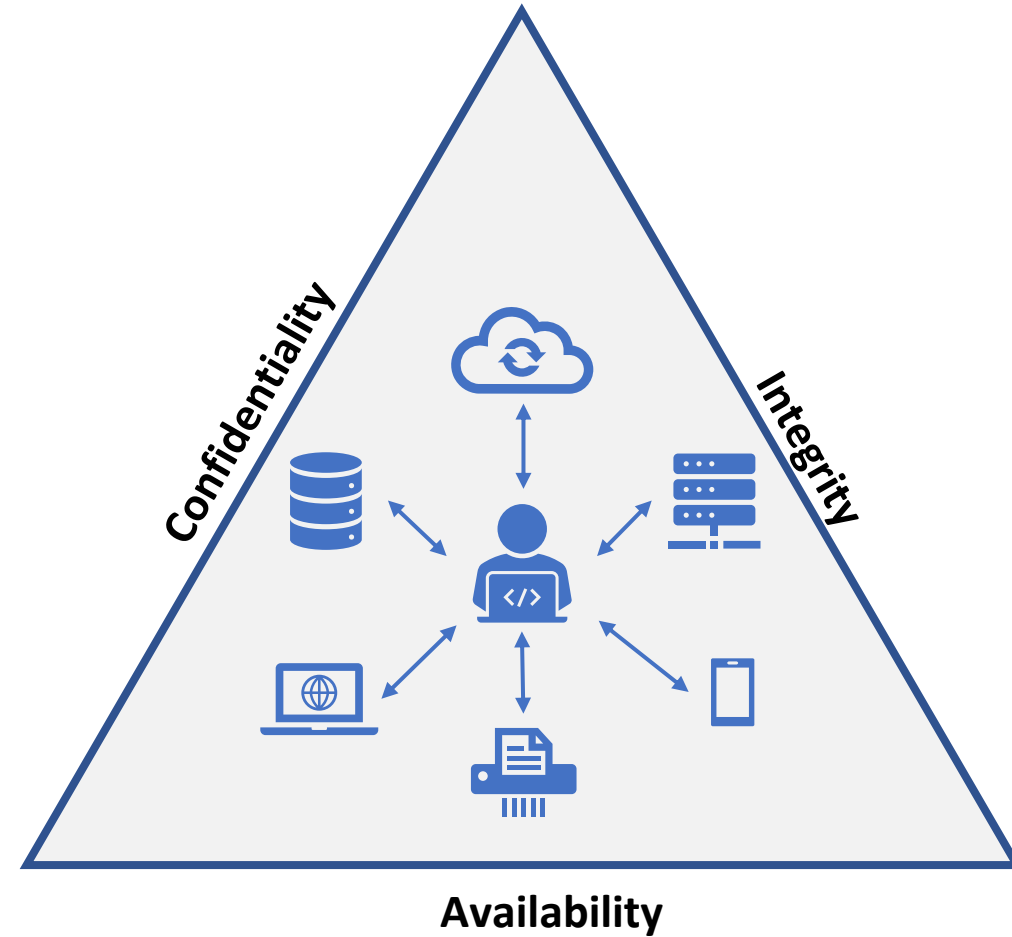


Human-Based

Threat actors who take actions to compromise the CIA of an organization.



Impact: Confidentiality, Integrity, and Availability



Definition: Threat

According to NIST, the term “**threat**” refers to “[a]ny circumstance or event with the potential to adversely impact organizational operations, organizational assets, individuals, other organizations, or the Nation through a system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.”

Source: [NIST SP 800-171 Rev. 1](#)



Threat Actors

THREAT ACTORS

HACKTIVISTS

Conduct attacks in furtherance of political interests.



CRIMINALS

Conduct attacks in furtherance of financial interests.



INSIDERS

Conduct attacks in furtherance of personal interests.

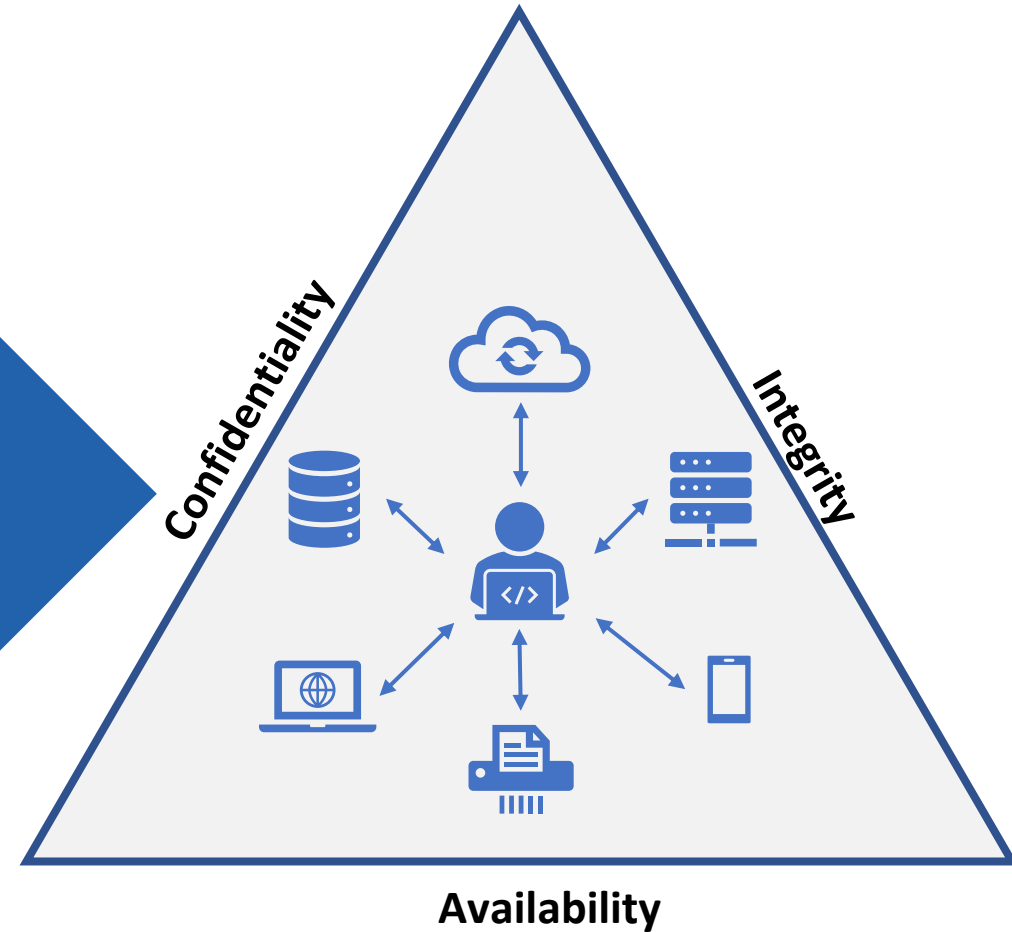


STATE ACTORS

Destruction, disruption, and espionage in furtherance of national interests.



Impact: Confidentiality, Integrity, and Availability



ODNI 2022 Annual Threat Assessment



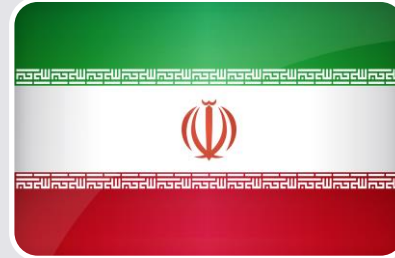
Russia - Remains a top cyber threat as it refines and employs its espionage, influence, and attack capabilities.

- Continues to target critical infrastructure, including underwater cables and industrial control systems.
- Considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.



China - Presents a prolific and effective cyber-espionage threat, possesses substantial cyber-attack capabilities, and presents a growing influence threat.

- Cyber pursuits and proliferation of related technologies increase the threats of cyber attacks against the US.
- Can cause localized, temporary disruptions to critical infrastructure within the US.



Iran - Expertise and willingness to conduct aggressive cyber operations make it a significant threat to the security of US networks and data.

- Has the ability to conduct attacks on critical infrastructure, as well as to conduct influence and espionage activities.
- Responsible for multiple cyber attacks against Israeli water facilities.

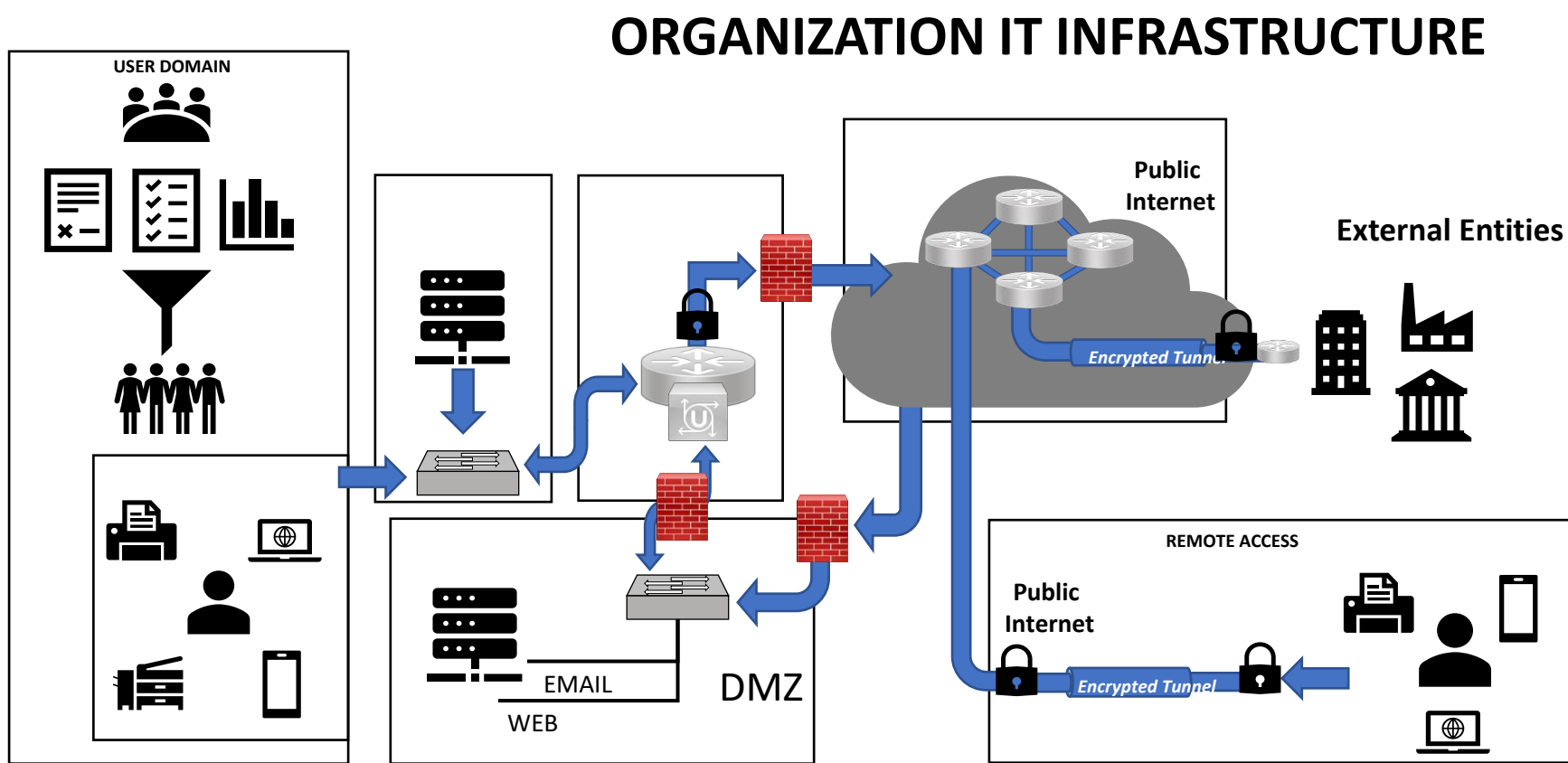


North Korea - Cyber program poses a growing espionage, theft, and attack threat.

- Possesses the expertise to cause temporary, limited disruptions of some critical infrastructure networks and disrupt business networks.
- Conducted cyber theft against financial institutions and cryptocurrency exchanges worldwide.



Cyber Attacks: Assets as Targets



THREAT ACTOR



Planning

- Identify target(s)

Discovery

- Identify target systems/users
- Identify vulnerabilities
- Identify exploits

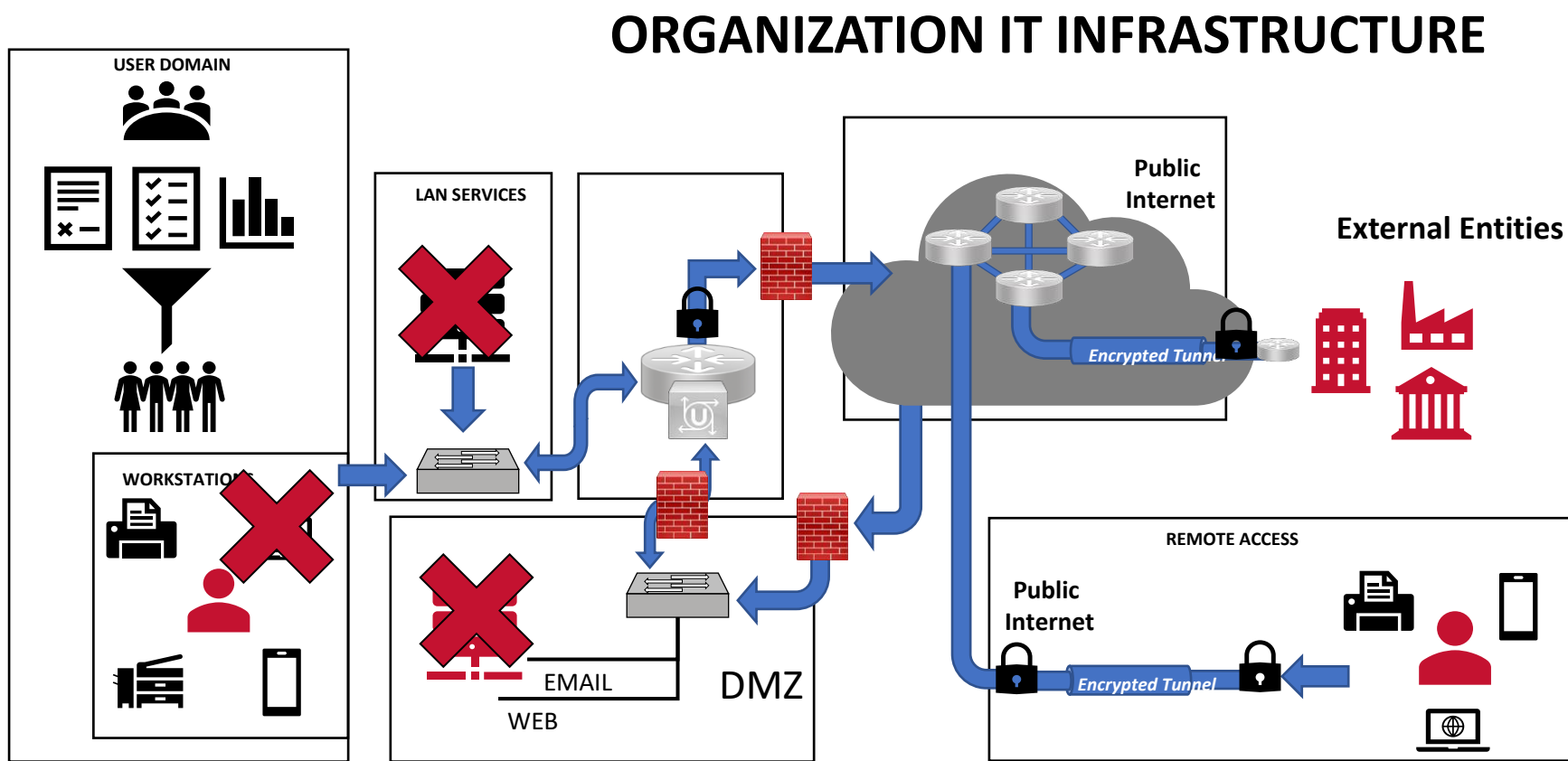
Attack

- Gain access
- Maintain access
- Hide tracks
- Accomplish attack goal



Prime Targets: Vulnerable Devices, Users, and Vendors

Cyber Attacks: Service Disruption



THREAT ACTOR



Planning

- Identify target(s)

Discovery

- Identify target systems/users
- Identify vulnerabilities
- Identify exploits

Attack

- Gain access
- Maintain access
- Hide tracks
- Accomplish attack goal



Attacks on Assets>Service Disruption>Mission Failure

Cyber Attacks: Attacks on Users

Social Engineering Attacks

■ Description:

- According to NIST, social engineering refers to “[t]he act of *deceiving an individual into revealing sensitive information, obtaining unauthorized access, or committing fraud by associating with the individual to gain confidence and trust.*”

Source: [NIST SP 800-63-3 Digital Identity Guidelines](#)

■ Threat Actor Objective:

- Manipulate a target (i.e., a user) into providing unauthorized access to information or information systems.

■ Common Threat Actor Techniques:

Phishing (Email-Based)

SMISHING (SMS-Based)

VISHING (Voice-Based)

Masquerading (In-Person/Physical)

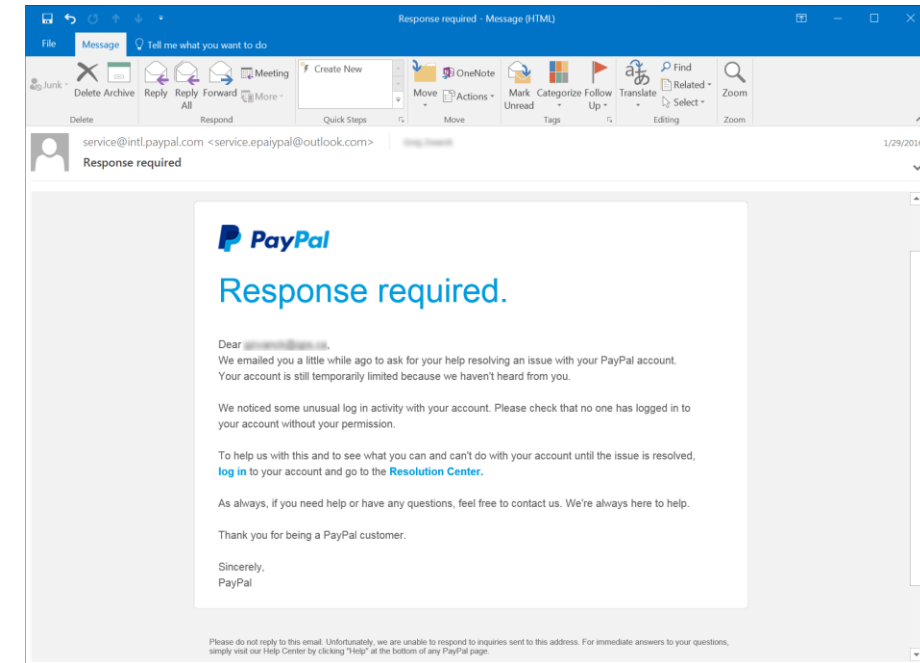


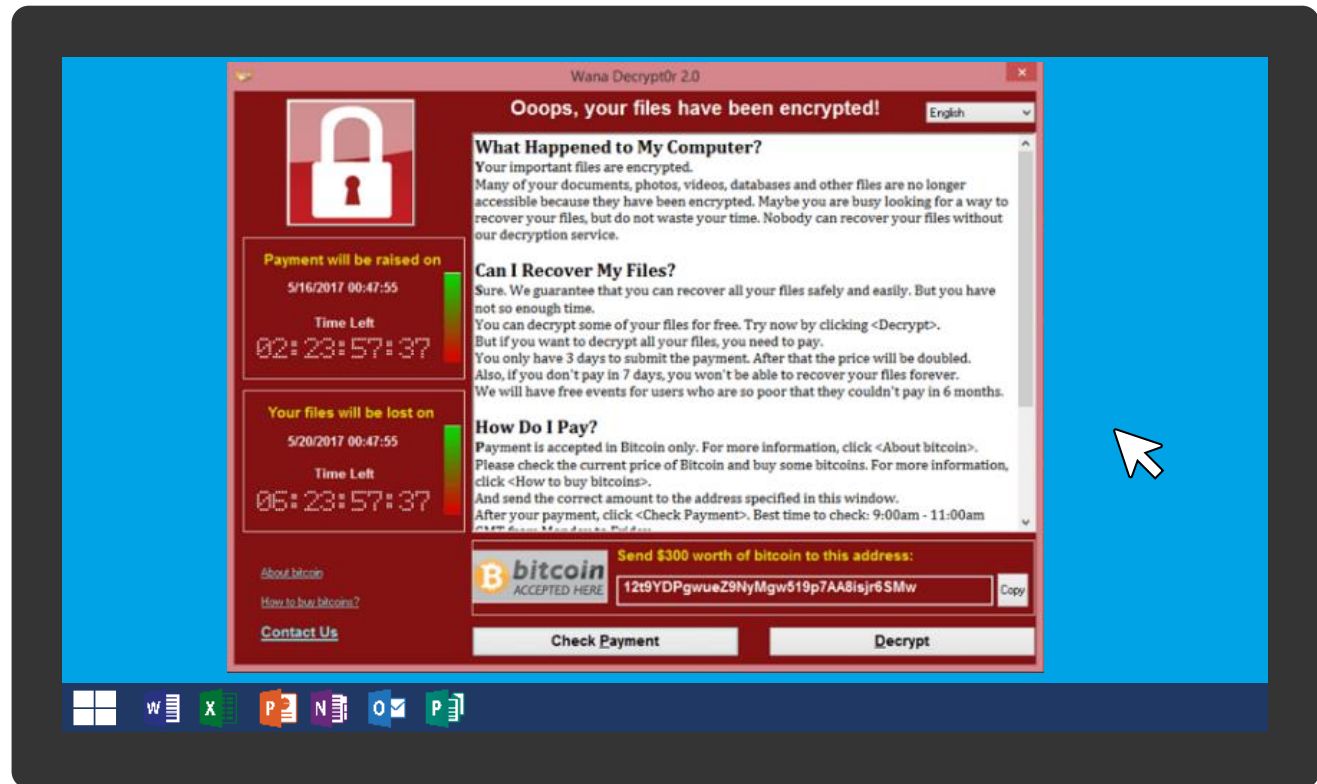
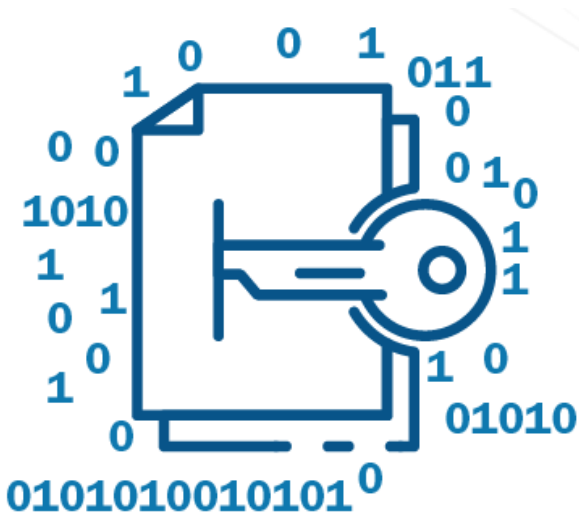
Image Source: knowbe4.com



Cyber Attacks: Ransomware

Ransomware Attacks

- **Ransomware:** the term “ransomware” refers to “a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable. Malicious actors then demand ransom in exchange for decryption.”
- **Source:** CISA Ransomware Guide 2020



Shields Up: Objective



<https://www.cisa.gov/shields-up>

Heightened Cybersecurity Posture

- Objective: Adopt a Heightened Cybersecurity Posture
- Near-Term Actions:
 1. Minimize Attack Surface
 - i. Reducing the likelihood of a damaging cyber intrusion
 2. Monitor and Protect Network
 - i. Detecting a potential cyber intrusion
 3. Incident Response: Exercise Your Plan
 - i. Prepare to respond to cyber intrusions
 4. Operational Resilience: Backups & Redundancy
 - i. Maximize operational resilience to a cyber incident
 5. See Something, Report Something



<https://www.cisa.gov/free-cybersecurity-services-and-tools>



<https://www.cisa.gov/shields-up>

Step 1: Minimize Attack Surface

Reduce the Likelihood of Damaging Cyber Intrusions



Minimize Attack Surface: Near-Term Steps

- Minimize Attack Surface and Harden Assets (Lock Doors & Windows)
 - Implement [Multi-Factor Authentication](#) for all accounts according to best practices
 - Enforce a strong password policy across the organization
 - Stop [Bad Practices](#)
 - End-of-Life Software, Default Accounts, Single-Factor Authentication
 - Update Software
 - Prioritize [known exploitable vulnerabilities](#) identified by CISA
 - System Hardening
 - Remove unnecessary accounts, ports, services, software on machines
 - Signup for [CISA's Cyber Hygiene Services](#) (External/Internet-Facing Scans)
 - Vulnerability Scanning
 - Web Application Scanning
 - Perform regular internal vulnerability scans
 - Run antivirus software throughout your network
 - Enable strong spam filters to prevent [phishing emails](#) from reaching end user
 - Train end users to identify, respond to, and report on phishing attacks



<https://www.cisa.gov/uscert/shields-technical-guidance>

Vulnerability Scanning Service (CyHy)

Assess Internet accessible systems for known vulnerabilities and configuration errors

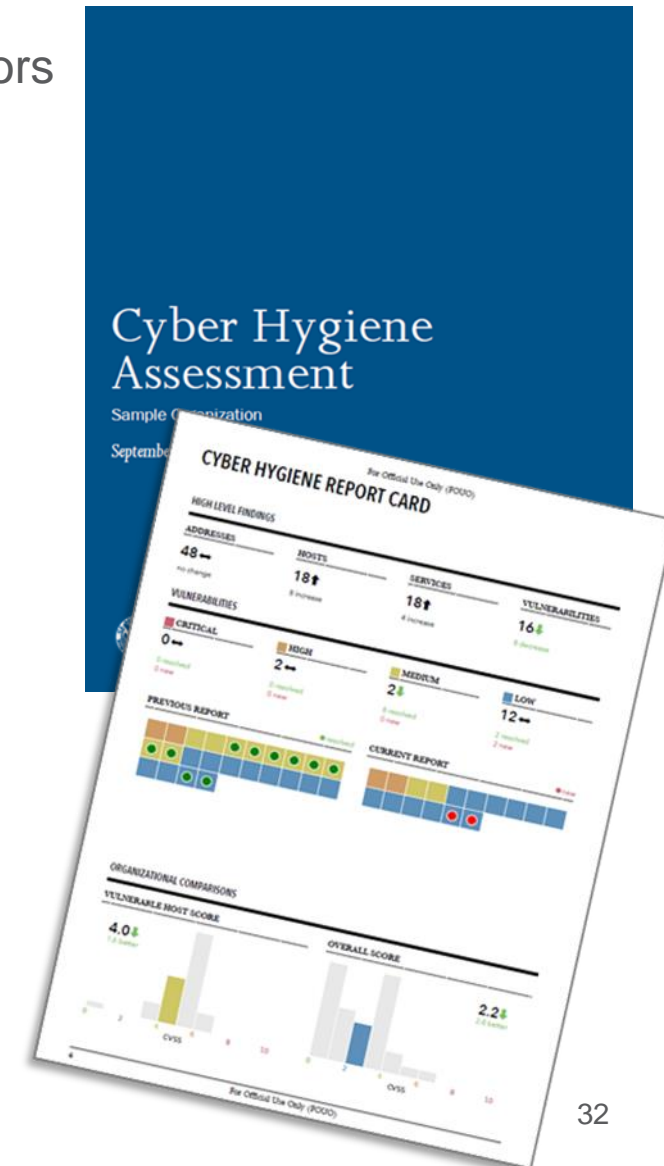
Work with organization to proactively mitigate threats and risks to systems

Activities include:

- Network Mapping
 - Identify public IP address space
 - Identify hosts that are active on IP address space
 - Determine the O/S and Services running
 - Re-run scans to determine any changes
 - Graphically represent address space on a map
- Network Vulnerability & Configuration Scanning
 - Identify network vulnerabilities and weakness



<https://www.cisa.gov/cyber-hygiene-services>



Step 2: Monitor and Protect

Take Steps to Quickly Detect a Potential Intrusion

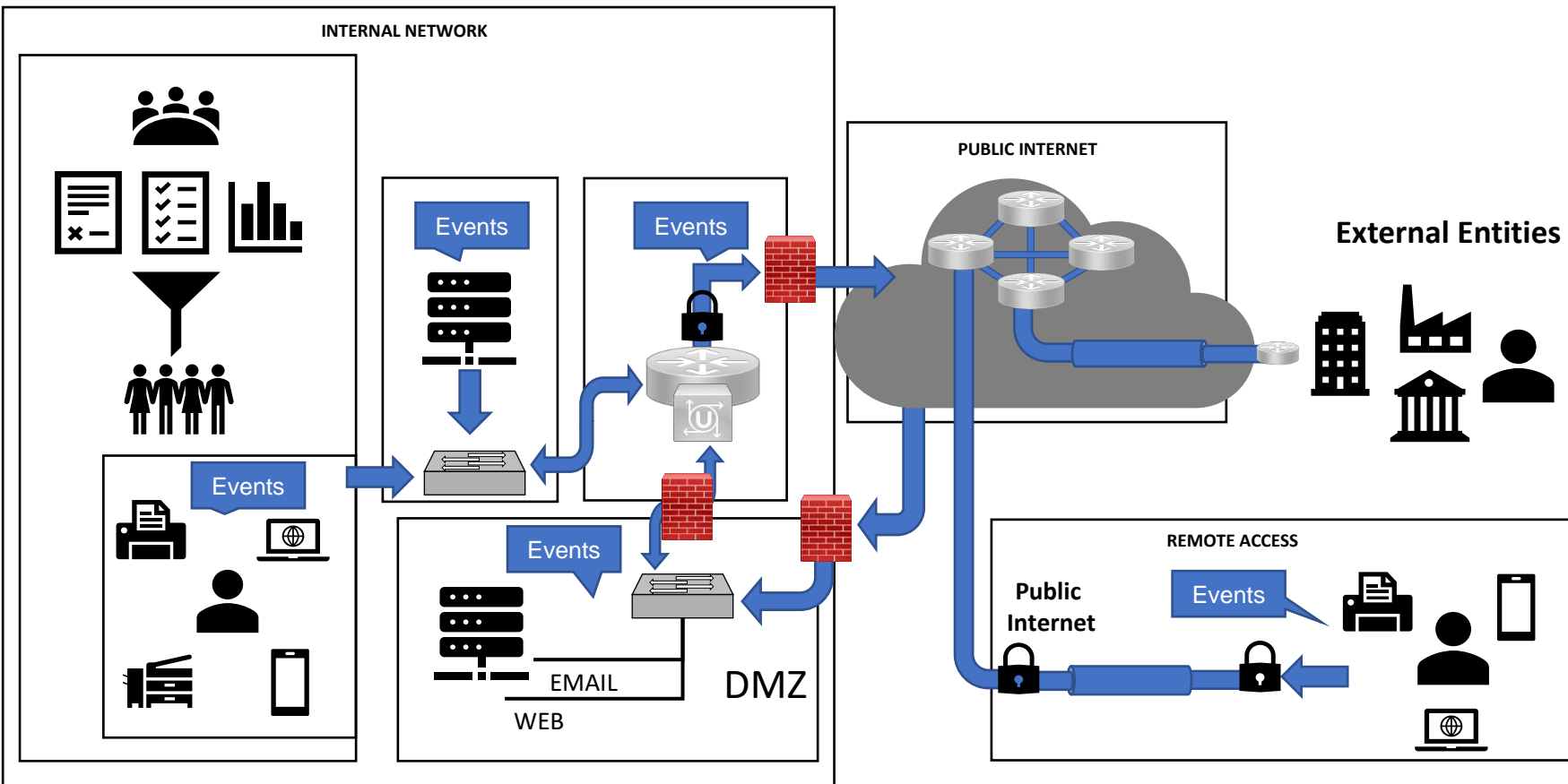


Monitor and Protect

- Monitor and Protect the Network: Near-Term Steps for “Heightened Security Posture”
 - Monitor your network for unusual behavior
 - Enable logging of events
 - Monitor hosts
 - Monitor network traffic
 - Monitor external vendors and/or contractors
 - Deploy host- and network-based anti-virus/anti-malware controls
 - Keep the signatures updated



What's an "event"?



Note: Events are generated by users and systems interacting with the technology assets in the organization's network. Most are imperceptible without specialized tools.



- **Event Defined:**

- An event is "one or more occurrences that affect organizational assets and have the **potential** to disrupt operations."
- An event may be any observable or measurable occurrence in the organization's systems or network

- **Event Examples:**

- Account login attempts
- File access
- File modification
- File deletion
- File transfers
- Remote access of internal resources
- Network traffic blocked at the firewall

Step 3: Incident Management

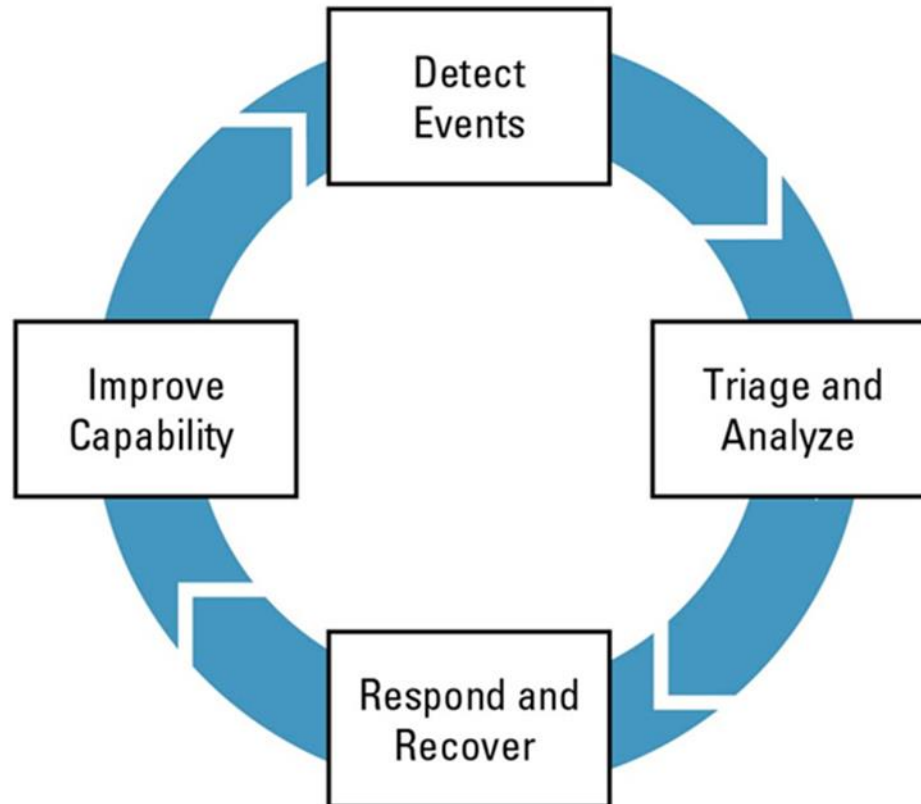
Be Prepared to Respond to Cyber Incidents



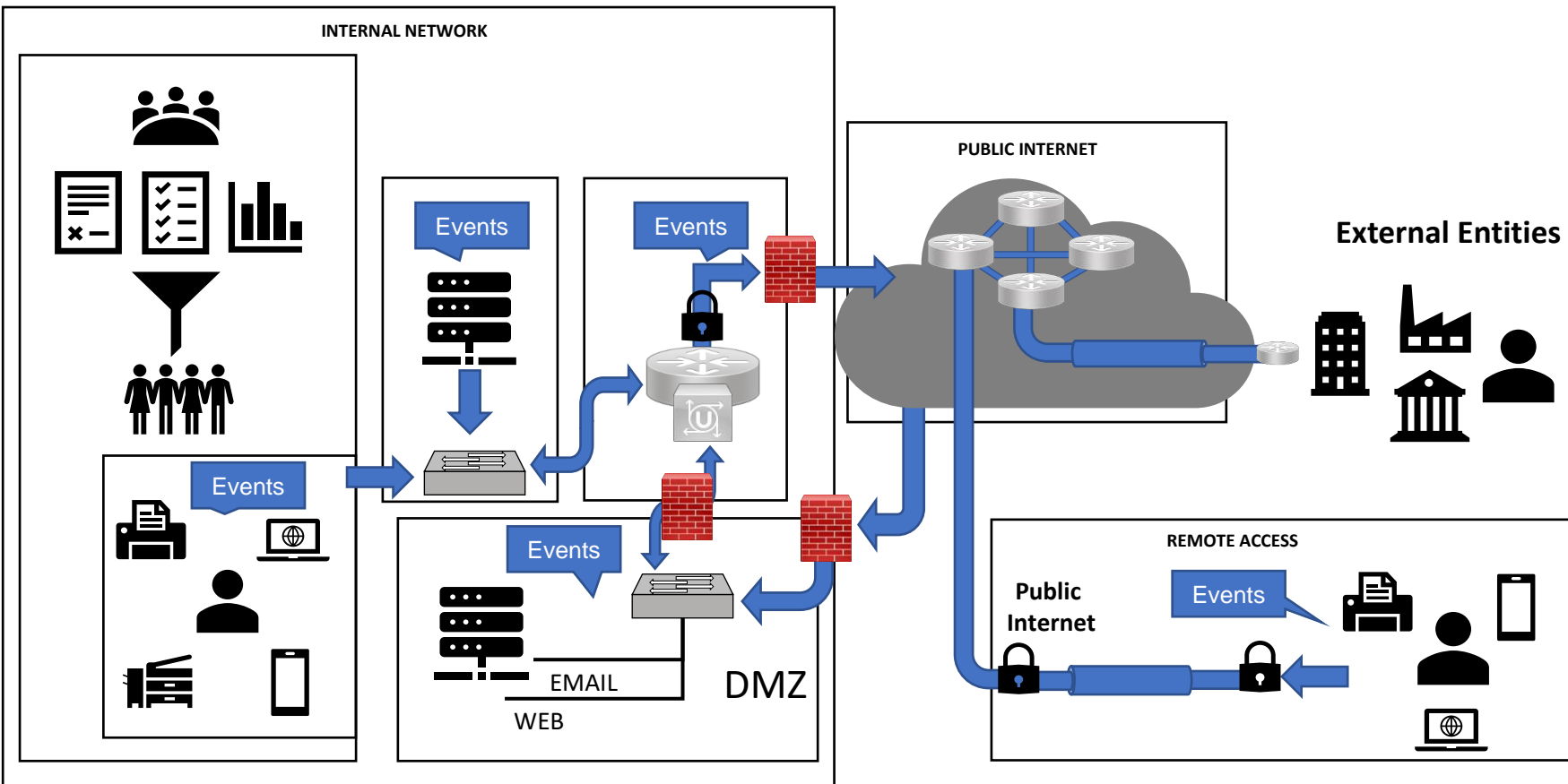
What is Incident Management?

The process of detecting, analyzing, responding to, and improving from disruptive events is known as **incident management**.

The **goal** of incident management is to mitigate the impact of a disruptive event.



What's an "event"?



- **Event Defined:**

- An event is "one or more occurrences that affect organizational assets and have the **potential** to disrupt operations."
- An event may be any observable or measurable occurrence in the organization's systems or network

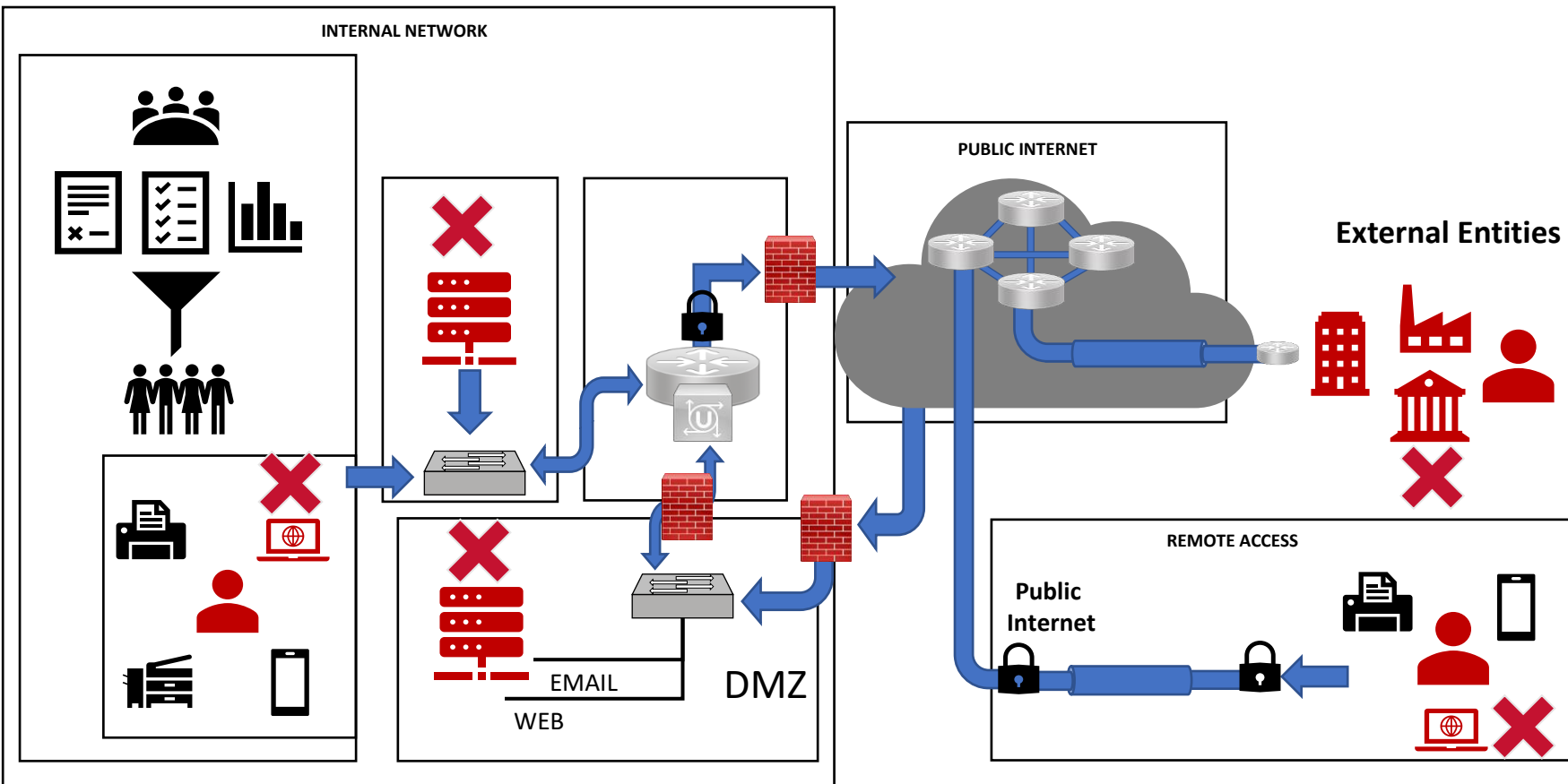
- **Event Examples:**

- Account login attempts
- File access
- File modification
- File deletion
- File transfers
- Remote access of internal resources
- Network traffic blocked at the firewall

Note: Events are generated by users and systems interacting with the technology assets in the organization's network. Most are imperceptible without specialized tools.



What's an "incident"?



Note: Organizations define the criteria of what qualifies as an incident. That criteria determines when an incident is declared. Once an incident is declared, the organization executes its incident response plan, in order to contain the impact, eradicate the threat, and recover the affected systems to a pre-incident state.



- **Incident Defined:**

- An incident is a high-magnitude event, or series of events, that:
 - Affects organizational operations;
 - Impacts the confidentiality, integrity, or availability of information systems;
 - Has a realized impact to operations; or
 - Requires a response in order to resume normal operations.

- **Incident Examples:**

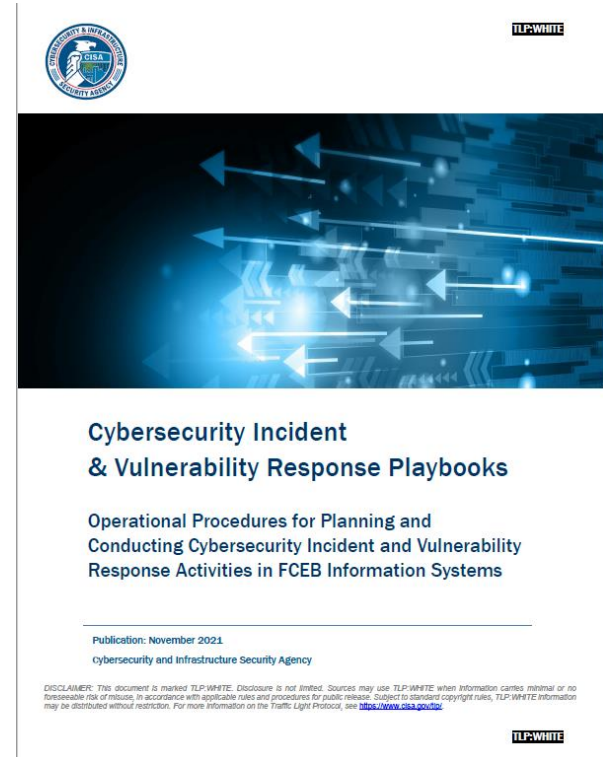
- Ransomware attack
- Unauthorized access of technology or information assets
- Denial of service attack

Incident Management: Near-Term Steps

- Incident Management/Response: Near-Term Steps for “Heightened Security Posture”
 - Designate an incident response team
 - Assure availability of key personnel
 - If you have an incident response plan – assess it with a [tabletop exercise](#)
 - If you **DO NOT** have an incident response plan – create one now
 - [CISA Ransomware Guide](#)
 - [Federal Government Cybersecurity Incident and vulnerability response playbooks](#)
 - CISA Incident Management Workshop
- CISA Ransomware Guide
 - Part 1: Ransomware Prevention Best Practices
 - Part 2: Ransomware Response Checklist



<https://www.cisa.gov/cisa-tabletop-exercises-packages>

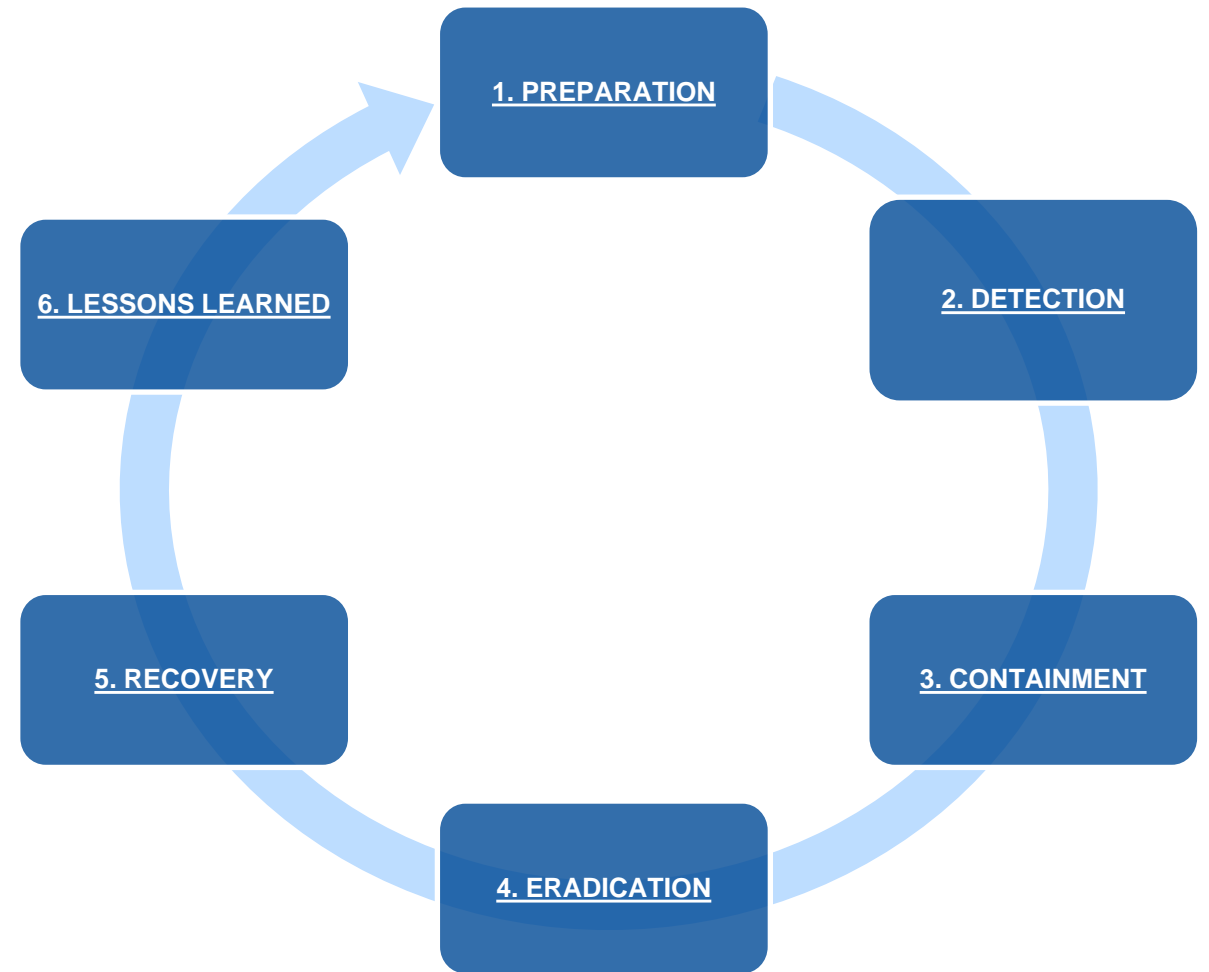


<https://www.cisa.gov/uscrt/ncas/current-activity/2021/11/16/new-federal-government-cybersecurity-incident-and-vulnerability>

What is an Incident Response Plan?

According to NIST, an **Incident Response Plan** is “[t]he documentation of a predetermined set of instructions or procedures to detect, respond to, and limit consequences of a malicious cyber attacks against an organization’s information system(s).”

Source: [NIST SP 800-34 Rev 1](#)



Example Incident Response process based off NIST SP 800-61r2



CISA Facilitated Tabletop Exercise

Description: A 3-hour non-technical facilitated cybersecurity tabletop exercise, where organizations are presented with a cyber threat-based scenario and are challenged to consider how their organization would respond, based on existing incident response plans.

Goal: The goal of the workshop is to provide organizations an opportunity to assess their level of readiness to respond to and recover from a cybersecurity incident impacting their operating environment.

Audience: Organizations that want to assess their level or readiness to respond to and recover from a cybersecurity incident.

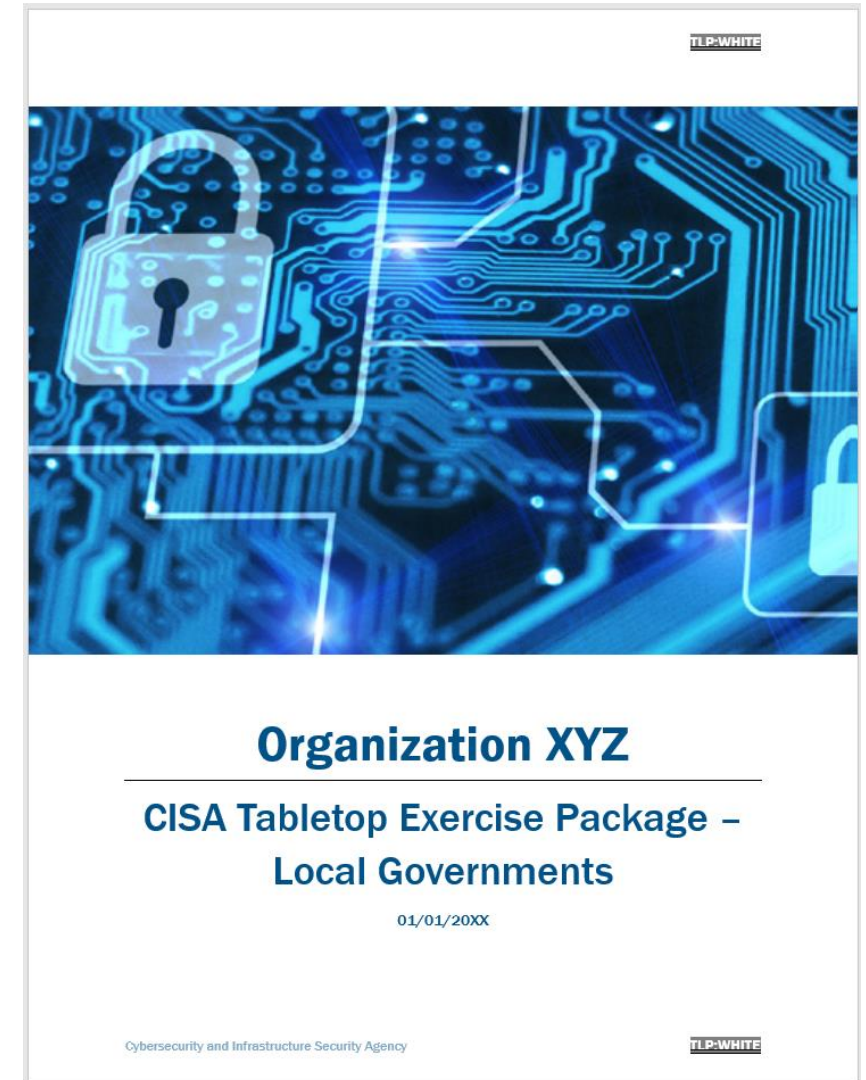
Format:

In-Person or Virtual

Key Topic: Incident Response, Incident Response Planning and Managing



Contact: ernesto.ballesteros@cisa.dhs.gov



Cyber Incident Management Workshop

Description: A 2-hour non-technical and informative session designed to help organizations understand incident management concepts, key elements, planning and implementation.

Goal: The goal of the workshop is to provide organizations with tangible, useful takeaway information on how to manage cybersecurity incidents effectively and, ultimately, achieve operational resilience.

Audience: Organizations that want to learn about an approach to developing a cyber incident management capability.

Format:

In-Person or Virtual

Key Topic: Incident Management, Incident Response Planning



Contact: ernesto.ballesteros@cisa.dhs.gov



CRR Supplemental Resource Guide



Volume 5

Incident Management

Version 1.1



Cyber Resilience Review (CRR):
Question Set with Guidance

February 2016



Step 4: Operational Resilience

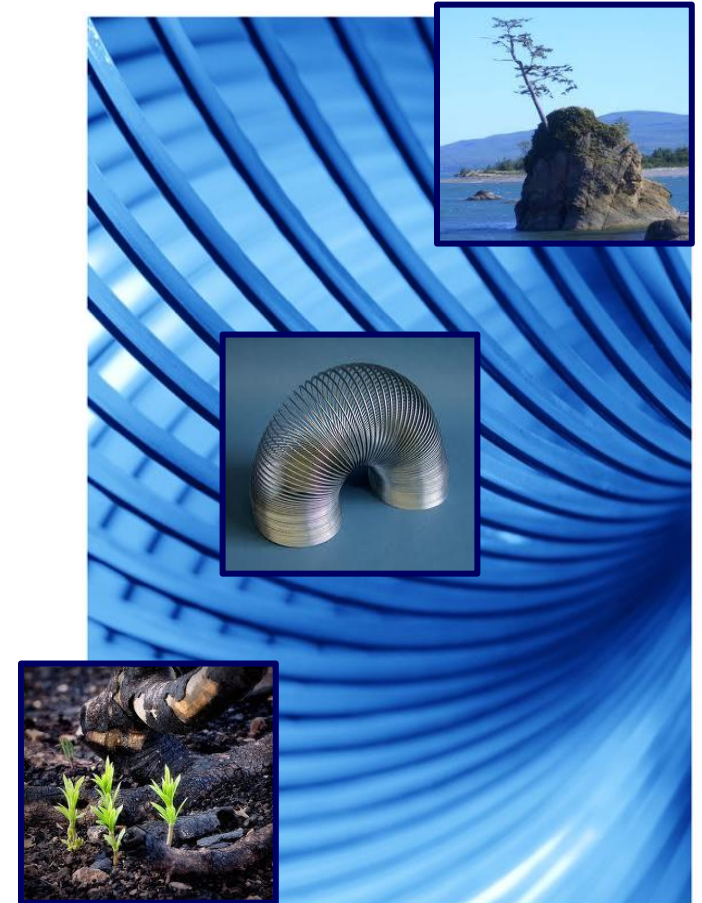
Maximize Organization Resilience to Destructive Cyber Incidents



What is Operational Resilience?

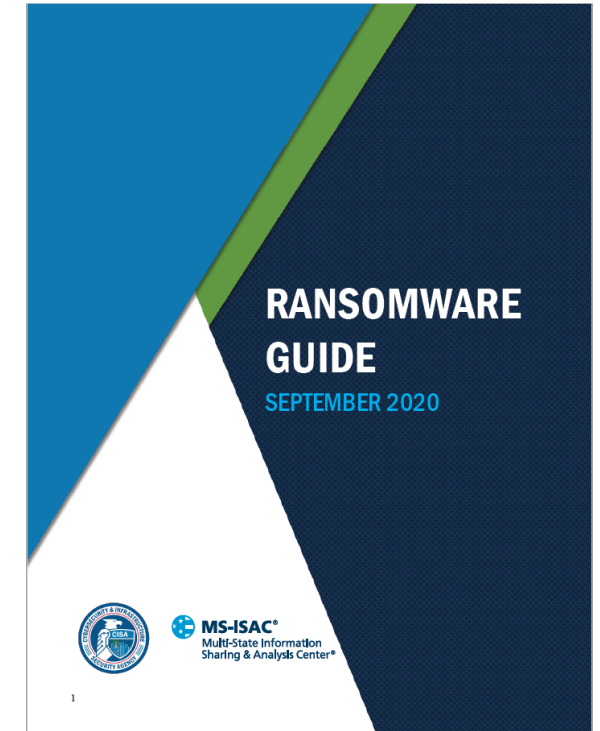
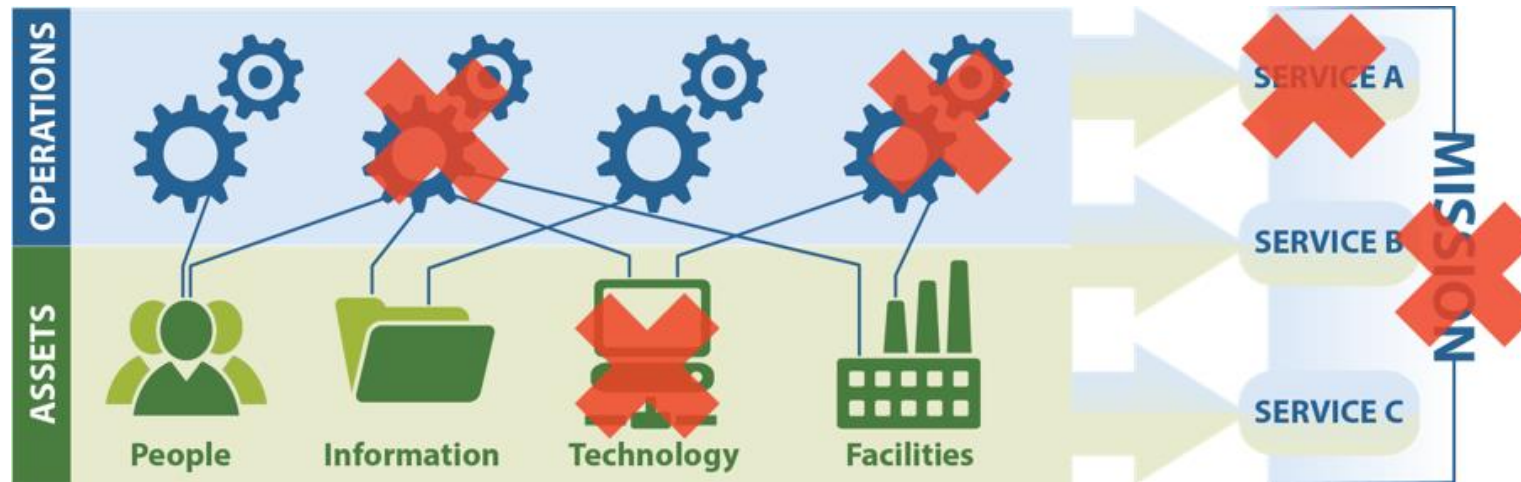
The emergent property of an organization that allows it to:

- Prevent disruptions from occurring
- Quickly respond to and recover from a disruption affecting its most critical business processes and services



Operational Resilience: Near-Term Steps

- Operational Resilience: Near-Term Steps for “Heightened Security Posture”
 - Backup mission-critical data, software, and “gold images”
 - Store backups off-line (preferably encrypted)
 - Test these backups
 - Acquire backup/redundant mission-critical hardware
 - Assess the readiness of your alternative/recovery site



<https://www.cisa.gov/stopransomware/ransomware-guide>



Cyber Resilience Review (CRR)

Purpose: The CRR is an assessment intended to evaluate an organization's operational resilience and cybersecurity practices of its critical services

Delivery: The CRR can be

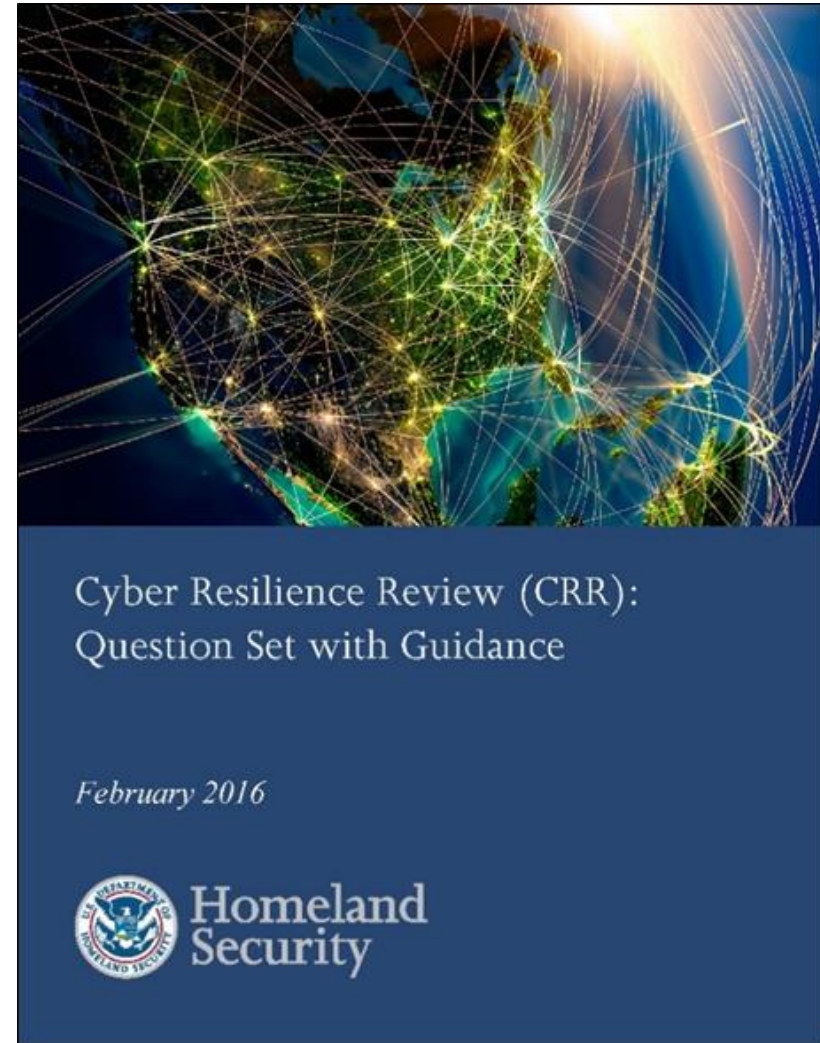
- Facilitated by CISA
- Self-administered

CRR Self-Assessment Package is available on the C-Cubed Voluntary Program website.

- Helps public and private sector partners understand and measure cyber security capabilities as they relate to operational resilience and cyber risk
- Based on the CERT ® Resilience Management Model (CERT® RMM)



Contact: ernesto.ballesteros@cisa.dhs.gov



Cyber Resilience Review (CRR) | Domains

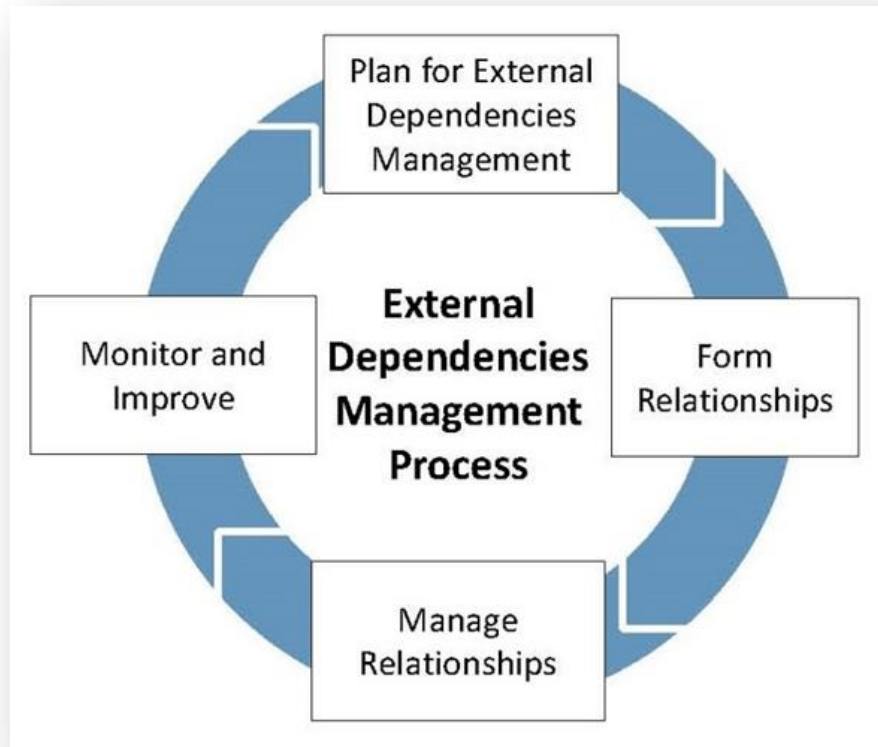
These represent key areas that typically contribute to an organization's cyber resilience— each domain focuses on:

- Documentation in place, and periodically reviewed & updated
- Communication and notification to all those who need to know
- Execution/Implementation & analysis in a consistent, repeatable manner
- Alignment of goals and practices within and across CRR domains

AM	Asset Management <i>identify, document, and manage assets during their life cycle</i>	SCM	Service Continuity Management <i>ensure continuity of IT operations in the event of disruptions</i>
CCM	Configuration and Change Management <i>ensure the integrity of IT systems and networks</i>	RISK	Risk Management <i>identify, analyze, and mitigate risks to services and IT assets</i>
CNTL	Controls Management <i>identify, analyze, and manage IT and security controls</i>	EXD	External Dependency Management <i>manage IT, security, contractual, and organizational controls that are dependent on the actions of external entities</i>
VM	Vulnerability Management <i>identify, analyze, and manage vulnerabilities</i>	TRNG	Training and Awareness <i>promote awareness and develop skills and knowledge</i>
IM	Incident Management <i>identify and analyze IT events, detect cyber security incidents, and determine an organizational response</i>	SA	Situational Awareness <i>actively discover and analyze information related to immediate operational stability and security</i>



External Dependency Management (EDM)



EDM process outlined in the External Dependencies Management Resource Guide



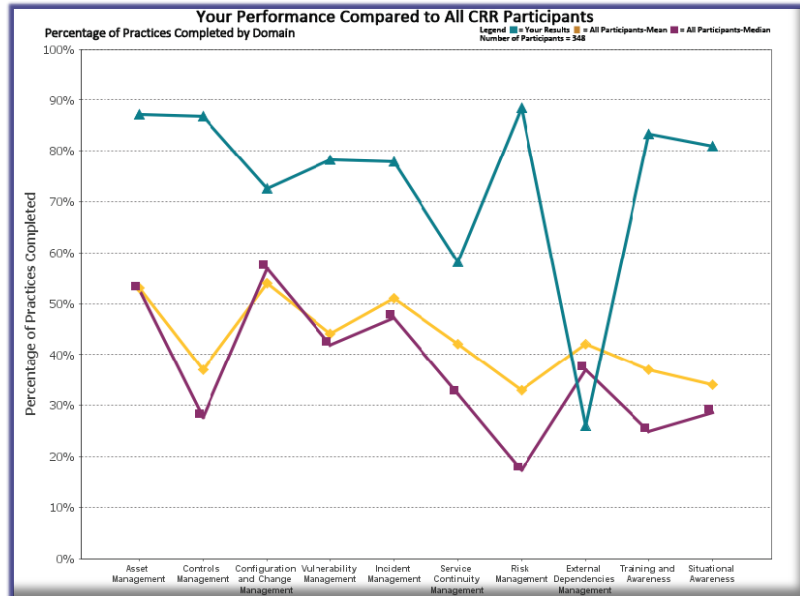
Contact: ernesto.ballesteros@cisa.dhs.gov

Overview: In 2016, DHS launched the External Dependencies Management (EDM) Assessment, focusing specifically on ensuring the protection and sustainment of services and assets that are dependent on the actions of third-party entities.

Background: External Dependencies Management is a domain covered by the CRR. However, EDM and associated issues (e.g., supply-chain management, vendor management) are not addressed at a comprehensive level within the CRR, resulting in the creation of a separate assessment.

Linkages to CRR: Despite operating at a more granular level than the CRR, the EDM Assessment borrows heavily from the CRR's methodological architecture and scoring system but remains a DHS-facilitated assessment.

Benefits of CRR and/or EDM Assessment



Comparison data with other CRR participants **facilitated only*



A summary “snapshot” graphic, related to the **NIST Cyber Security Framework**.

Domain performance of existing cybersecurity capability and options for consideration for all responses

DOMAIN 1: ASSET MANAGEMENT

MIL-1					MIL-3					MIL-4					MIL-5				
G1	G2	G3	G4	G5	G6	G7	G8	G9	G10	G11	G12	G13	G14	G15	G16	G17	G18	G19	G20

The purpose of Asset Management (AM) is to identify, document, and manage assets during their life cycle to ensure sustained productivity to support critical services. There are seven goals in Asset Management:

- Goal 1 – Identify & prioritize critical services
- Goal 2 – Inventory assets, and establish the authority and responsibility for these assets
- Goal 3 – Establish the relationship between assets and the services they support
- Goal 4 – Manage the asset inventory
- Goal 5 – Manage access to assets
- Goal 6 – Prioritize & manage information assets
- Goal 7 – Prioritize & manage facility assets

The following contains questions asked during the CRR for each goal in the Asset Management domain, and your organization's response to these questions. In cases where the response is noted as "Incomplete" or "No", there is an accompanying Option for Consideration addressing that question.

Goal 1 – Identify & prioritize critical services		
1.	Are critical services identified? [SC.SG2.SP1]	Yes
2.	Are critical services prioritized based on analysis of potential impact if these services are disrupted? [SC.SG2.SP1]	Incomplete
Q2 CERT-RMM Reference: [SC.SG2.SP1] Identify and inventory critical services, associated assets, and activities. A fundamental risk management principle is to focus on activities to protect and sustain services and assets that most directly affect the organization's ability to achieve its mission. Additional Reference: NIST SP 800-34, Revision 1 "Contingency Planning Guide for Federal Information Systems" (pages 15-18)		

Goal 2 – Inventory assets, and establish the authority and responsibility for these assets		
1.	Are the assets that directly support the critical service inventoried? [ADM.SG1.SP1]	Incomplete
	People	Incomplete
	Information	Incomplete
	Technology	Incomplete
	Facilities	Yes
Q1 CERT-RMM Reference: [ADM.SG1.SP1] Identify and inventory critical assets. An organization must be able to identify its critical assets, document them, and establish their value in order to develop strategies for protecting and sustaining assets commensurate with their value to the services they support. Additional Reference: NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems" (pages 2-3)		



Step 5: See Something -- Report Something

Lower Reporting Thresholds



See Something – Report Something

See Something – Report Something



Report Incidents



Report Phishing



Report Malware



Report Vulnerabilities



Share Indicators

Organizations should report anomalous cyber activity and/or cyber incidents 24/7 to report@cisa.gov or (888) 282-0870.



<https://www.cisa.gov/uscert/report>

Incident Reporting

CISA Incident Reporting System

Report incidents that include:

1. Attempts to gain unauthorized access to a system or its data;
2. Unwanted disruption or denial of service; or
3. Abuse or misuse of a system or data in violation of policy.



Report Incidents

CISA's 24x7 contact number: 888-282-0870 | report@cisa.gov

FBI's 24x7 CyWatch: 855-292-3937 | CyWatch@fbi.gov



<https://us-cert.cisa.gov/forms/report>

Shields Up: Remain Vigilant



<https://www.cisa.gov/shields-up>

Next Steps

Forming a Partnership with CISA Pre-Incident



No-Cost Cyber Resources and Assessments

Regional Cybersecurity Resources:

- Cybersecurity Assessments (*Performed by Cybersecurity Advisors*)
 - Introductory Level:
 - Ransomware Readiness Assessment (RRA)
 - Cybersecurity Performance Goals Assessment (CPG)
 - Intermediate Level:
 - Cyber Infrastructure Survey (CIS)
 - Advanced Level:
 - Cyber Resilience Review (CRR)
 - External Dependencies Management (EDM)
 - Incident Management Review (IMR)
- Cybersecurity Exercises and Workshops (*Performed by Cybersecurity Advisors*)
 - Cyber Resilience Workshop (CRW)
 - Incident Management Workshop (IMW)
 - Vulnerability Management Workshop (VMW)
 - Intro to Digital Forensics Workshop (DFW)
 - Facilitated Cyber Exercise (FCE)

National/Automated Cybersecurity Resources:

- Vulnerability Scanning Service (CyHy)



Next Steps: Partnership Formation

Would you like to know more about CISA's no-cost cyber resources and partnership opportunities?

Next Steps:

1. Contact your CISA Regional Office ([Region Offices](#));
2. Request an initial Cyber Protective Visit (CPV) from your Cybersecurity Advisor (CSA) or State Cybersecurity Coordinator (CSC); and
3. Explore discuss how CISA can assist you in assessing and managing your organization's cybersecurity risk.



<https://www.cisa.gov/cisa-regions>

Additional Resources

- [CISA Shields Up Webpage](#)
- [CISA's Cross-Sector Cybersecurity Performance Goals](#)
- [CISA Catalog of Free Cybersecurity Services](#)
- [CISA Cyber Resource Hub](#)
- [CISA's Free Cybersecurity Services and Tools Webpage](#)



<https://www.cisa.gov/free-cybersecurity-services-and-tools>





CISA REGION 6

**Ernesto Ballesteros, JD, MS, CISSP,
CISA, Security+**

Cybersecurity State Coordinator of Texas, Region 6
Cybersecurity and Infrastructure Security Agency

EMAIL: ernesto.ballesteros@cisa.dhs.gov

CELL: (210) 202-6646

CISA Region 6

CISARegion6@hq.dhs.gov

CISA INCIDENT REPORTING SYSTEM

<https://us-cert.cisa.gov/forms/report>

CISA CENTRAL - 24/7 Watch

(888) 282-0870; report@cisa.gov

FBI's 24/7 Cyber Watch (CyWatch) ⁶⁸

(855) 292-3937; CyWatch@fbi.gov