

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY



Cybersecurity and Infrastructure Security Agency (CISA)

VISION

Secure and resilient
infrastructure for the
American people.

MISSION

We lead the National effort
to understand, manage, and
reduce risk to our cyber and
physical 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

Our Work

The Cybersecurity and Infrastructure Security Agency (CISA) works 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



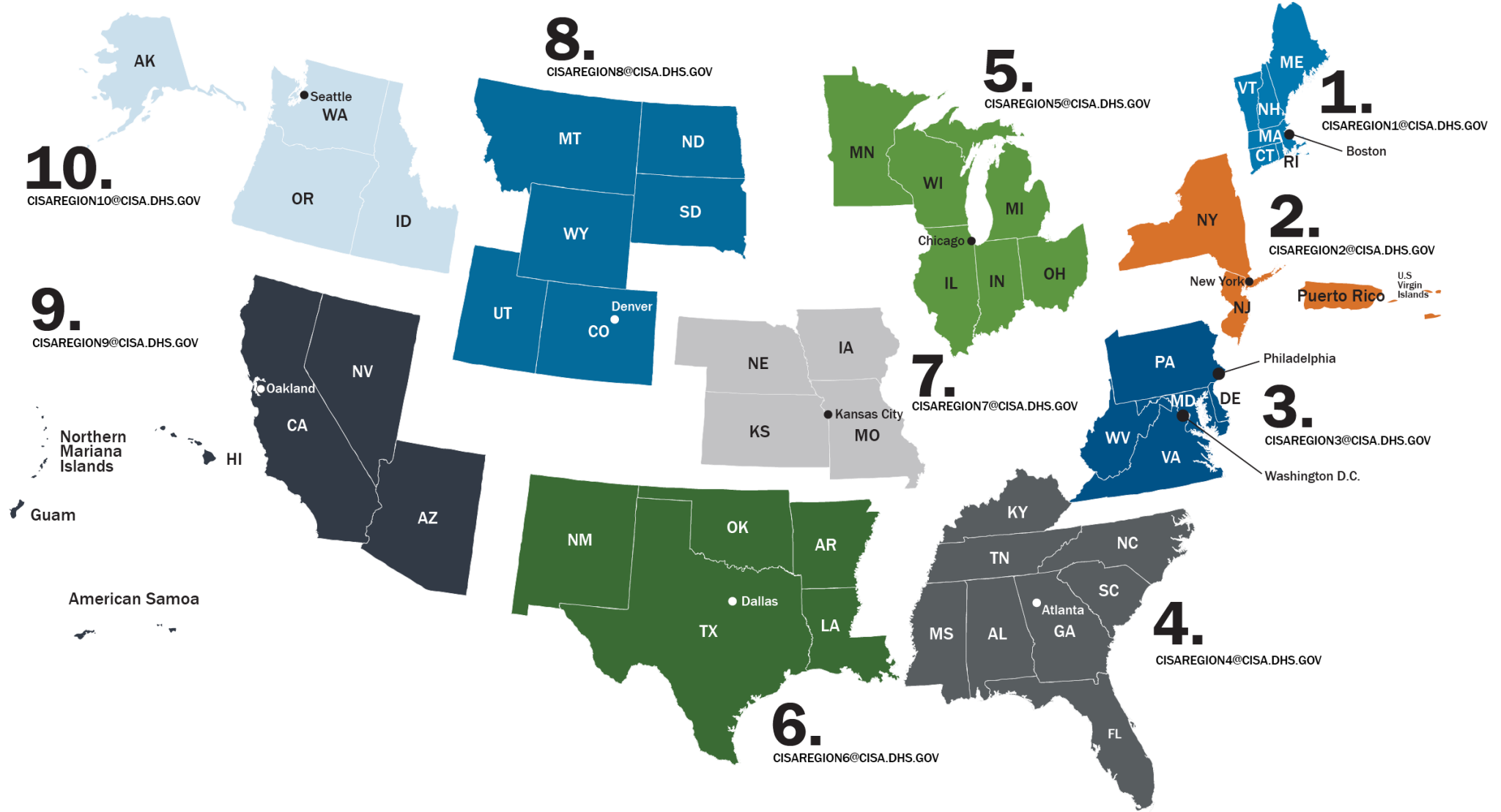
EMERGENCY
COMMUNICATIONS

16 Critical Infrastructure Sectors & Corresponding Sector Risk Management Agencies

 CHEMICAL	CISA	 FINANCIAL	Treasury
 COMMERCIAL FACILITIES	CISA	 FOOD & AGRICULTURE	USDA & HHS
 COMMUNICATIONS	CISA	 GOVERNMENT FACILITIES	GSA & FPS
 CRITICAL MANUFACTURING	CISA	 HEALTHCARE & PUBLIC HEALTH	HHS
 DAMS	CISA	 INFORMATION TECHNOLOGY	CISA
 DEFENSE INDUSTRIAL BASE	DOD	 NUCLEAR REACTORS, MATERIALS AND WASTE	CISA
 EMERGENCY SERVICES	CISA	 TRANSPORTATIONS SYSTEMS	TSA & USCG
 ENERGY	DOE	 WATER	EPA

CISA Regions

- 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



Joint Cyber Defense Collaborative (JCDC)

Reduce risk to critical infrastructure and National Critical Functions

- Integration of public-private sector cyber defense planning
- Information fusion
- Cybersecurity guidance production & dissemination

Akamai

AT&T

AWS

Broadcom

Cisco

Cloudflare

Crowdstrike

Google Cloud

IBM

Juniper

Lumen

Mandiant

Microsoft

Oracle

Palo Alto Networks

SecureWorks

Splunk

Tenable

Trellix

Verizon

VMware

CISA

NCD

DNI

FBI

NSA

USSS

DoD

DoJ



Today's Risk Landscape

America remains at risk from a variety of threats:



ACTS OF TERRORISM



CYBER ATTACKS



EXTREME WEATHER



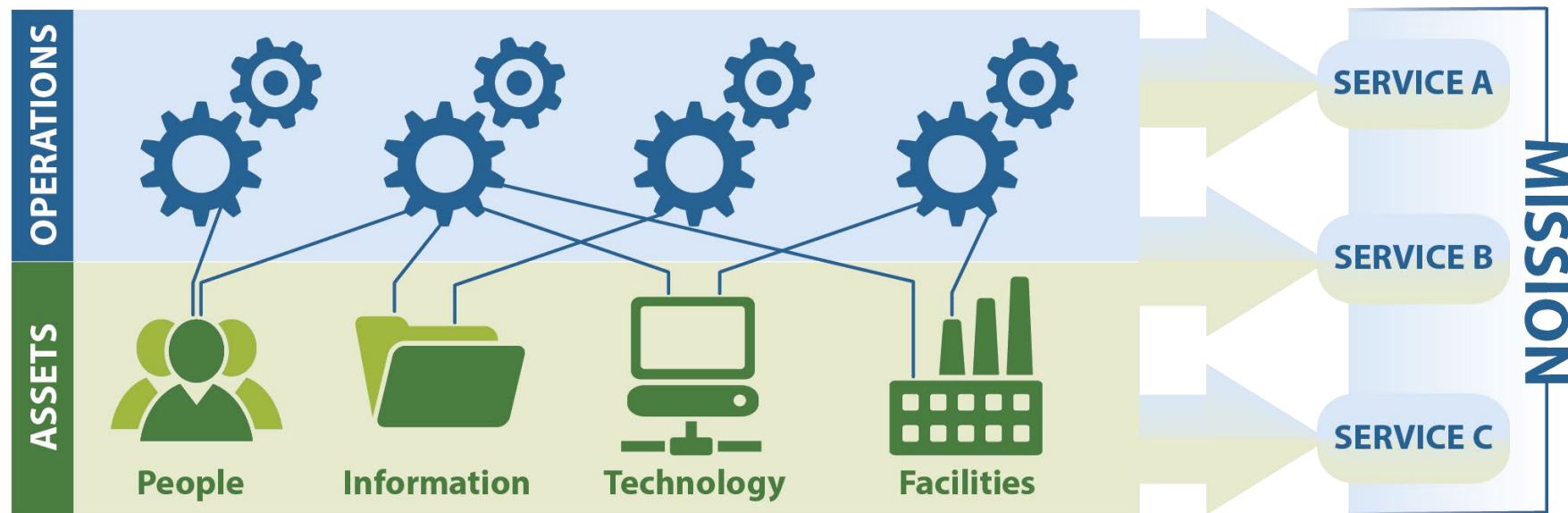
PANDEMICS



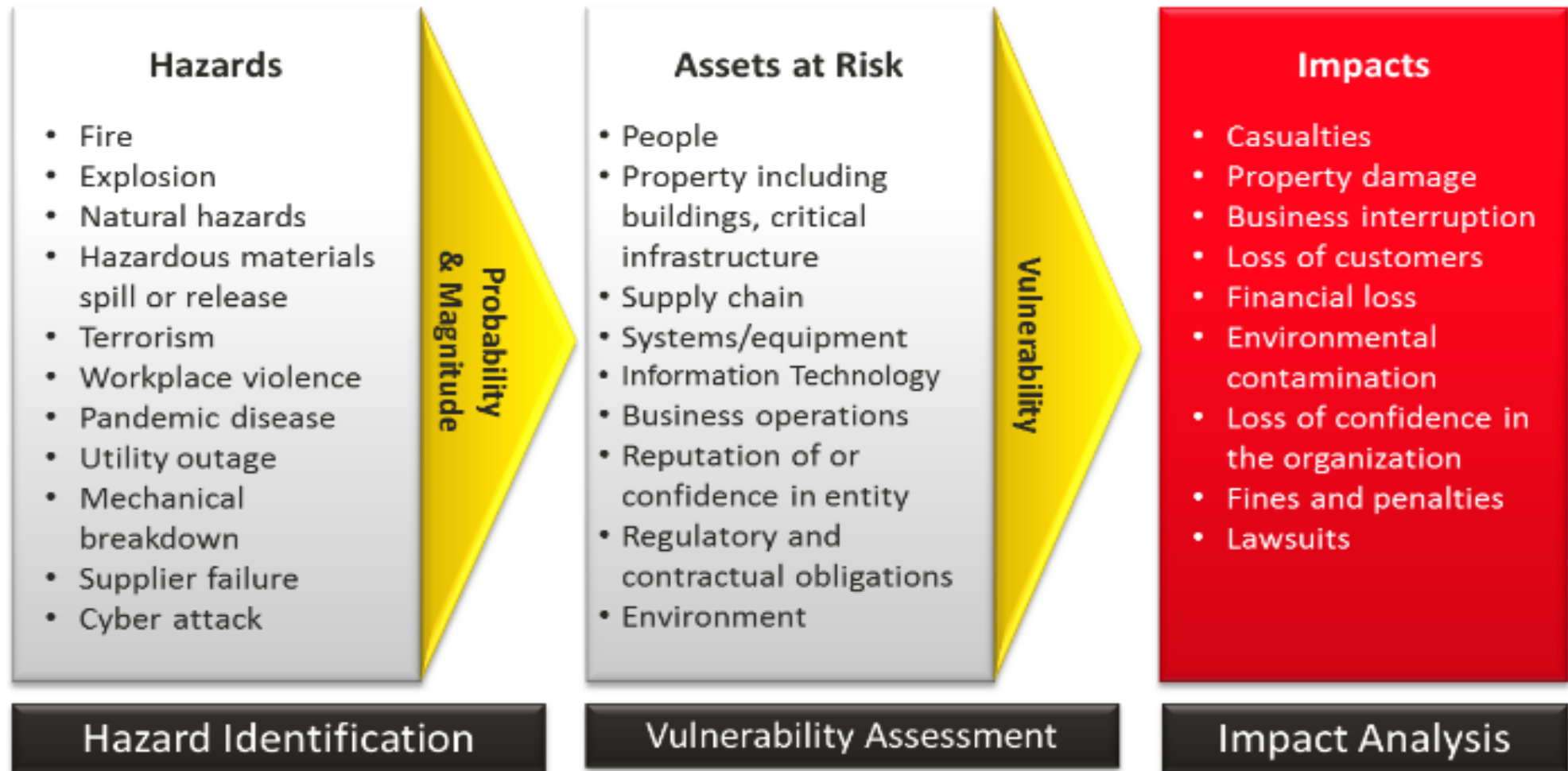
ACCIDENTS
OR TECHNICAL
FAILURES

Defining the Critical Services

An organization uses its **assets (people, information, technology, and facilities)** to provide operational **services** for accomplishing the organization's **mission**.



Hazards – Risk - Impacts

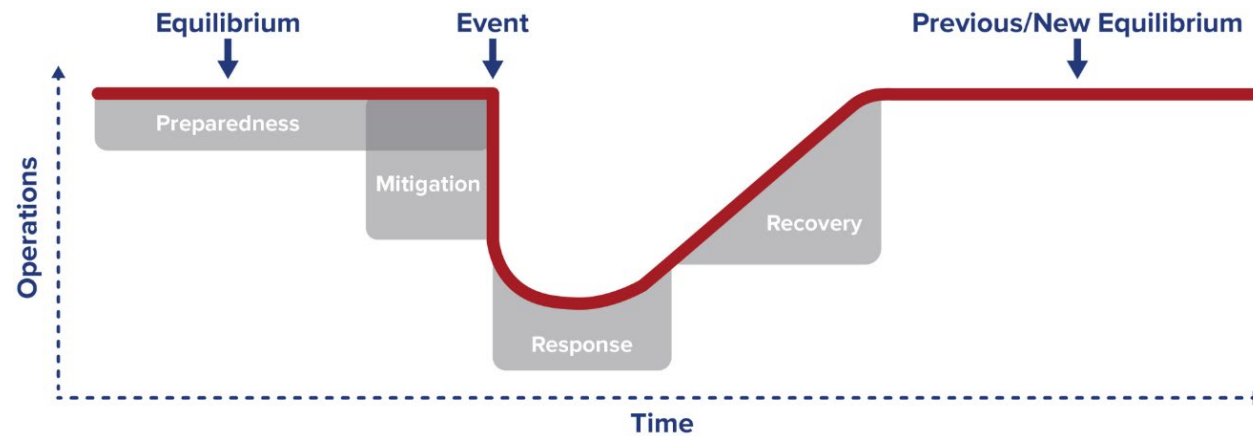


**Notional graphic ; lists are not all encompassing*



Risk Management Strategies

- Preparedness (Prevention, Protection)
- Mitigation
- Response
- Recovery



Security Advisor Programs

Security Advisors are field-based critical infrastructure security specialists who link State, local, tribal, territorial (SLTT) & private sector stakeholders with infrastructure protection resources

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

Protective Security Advisors (PSA): Security, Emergency Preparedness, and Business Continuity Programs

Cybersecurity Advisors (CSA): Cybersecurity for Information Technology & Operational Technology networks



Protective Security Advisors

Protective Security Advisors (PSAs):

- Plan, coordinate, and conduct security and resiliency surveys and assessments
- Plan and conduct outreach activities
- Support National Special Security Events (NSSEs) and Special Event Activity Rating (SEAR) events
- Provide vital link for information sharing during steady state and incident response
- Coordinate and support risk mitigation training



PSA Assessments



Security Walk-Through Assessment

- Programs Reviewed
 - Security
 - Emergency Preparedness
 - Business Continuity
- Time Requirement = Site Dependent; Tour of facility(s) followed by conference room meeting
- Written report **NOT** provided

Security Assessment at First Entry (SAFE)

- Programs Reviewed
 - Security
 - Emergency Preparedness
 - Business Continuity
- Time Requirement = Site Dependent; Tour of facility(s) followed by conference room meeting
- Written report provided

Infrastructure Survey Tool (IST)

- Programs Reviewed
 - Security
 - Emergency Preparedness
 - Business Continuity
 - Dependencies/Interdependencies
 - Information Technology
- Time Requirement = Typically two full days
- Written report provided



Cybersecurity Advisors

Cybersecurity Advisors (CSAs):

- Advise FSLTT and private sector partners on risk levels, security posture, & cost-benefit analysis of information security programs & processes
- Review risk management programs by using evaluation results to create or enhance the effectiveness of the partner's information sharing
- Reduce risks to the nation's critical cyber infrastructure by delivering key mitigation capabilities
- Promote collaborative efforts to reduce risks and threats to critical information, enterprise, communications, and control systems
- Plan and conduct outreach activities relating to cybersecurity initiatives
- Build regional and local cybersecurity coalitions to promote information sharing



Cyber Services Planning - Initial

Step One

Cyber Protective Visit (CPV):

- Initial visit with a Cyber Security Advisor (CSA) to gauge interest in CISA services, understand the organization's needs, and develop the foundation for further engagements and offerings.

Step Two

Cyber Hygiene Vulnerability Scanning (CyHy):

- Maintain enterprise awareness of your internet-accessible systems
- Provide insight into how systems and infrastructure appear to potential attackers
- Drive proactive mitigation of vulnerabilities and reduce risk

Step Three

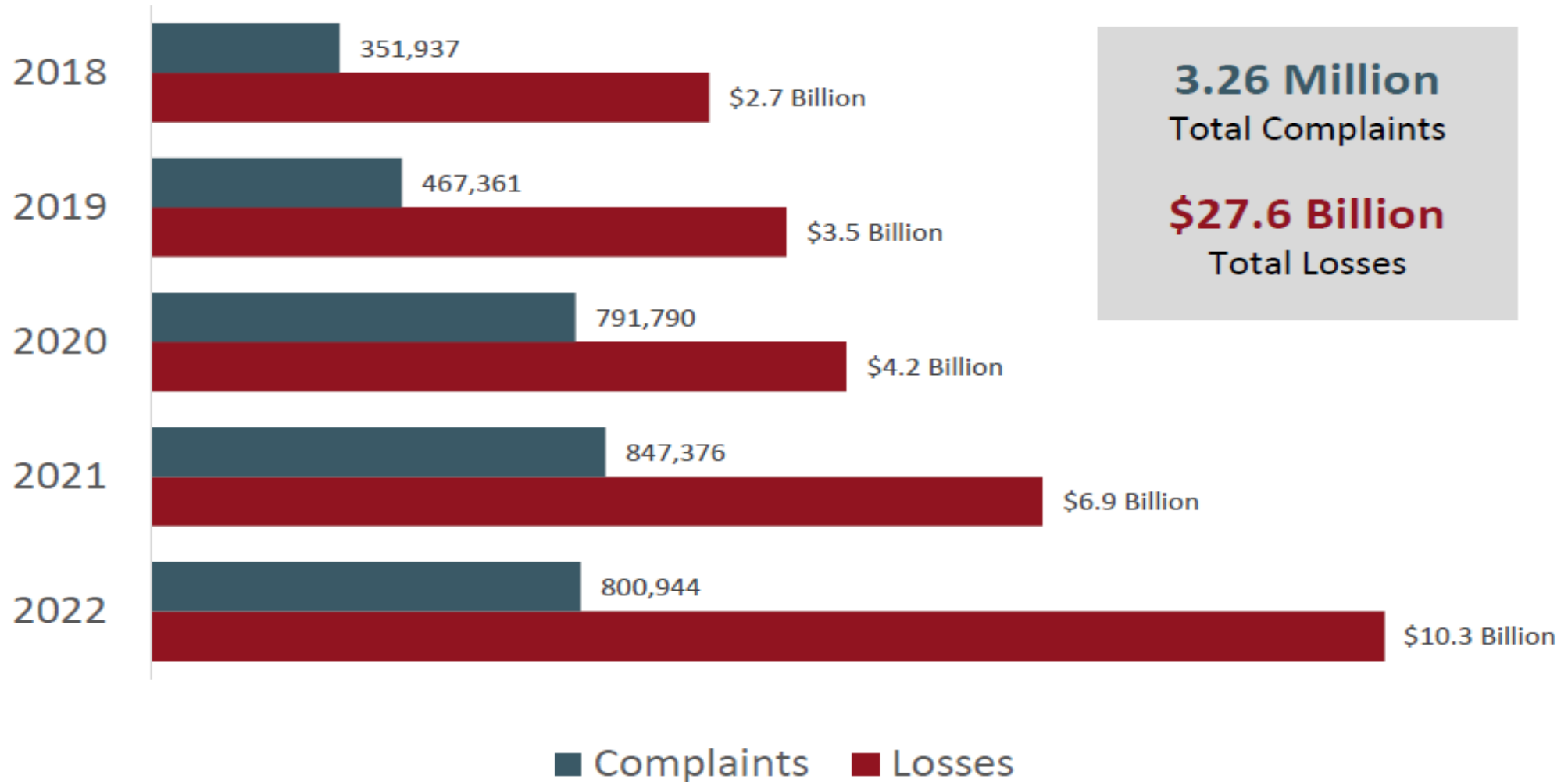
Ongoing Partnership:

- Information sharing
- Assessments
- Tabletop Exercises
- Presentations
- Connection to resources
- Incident Support

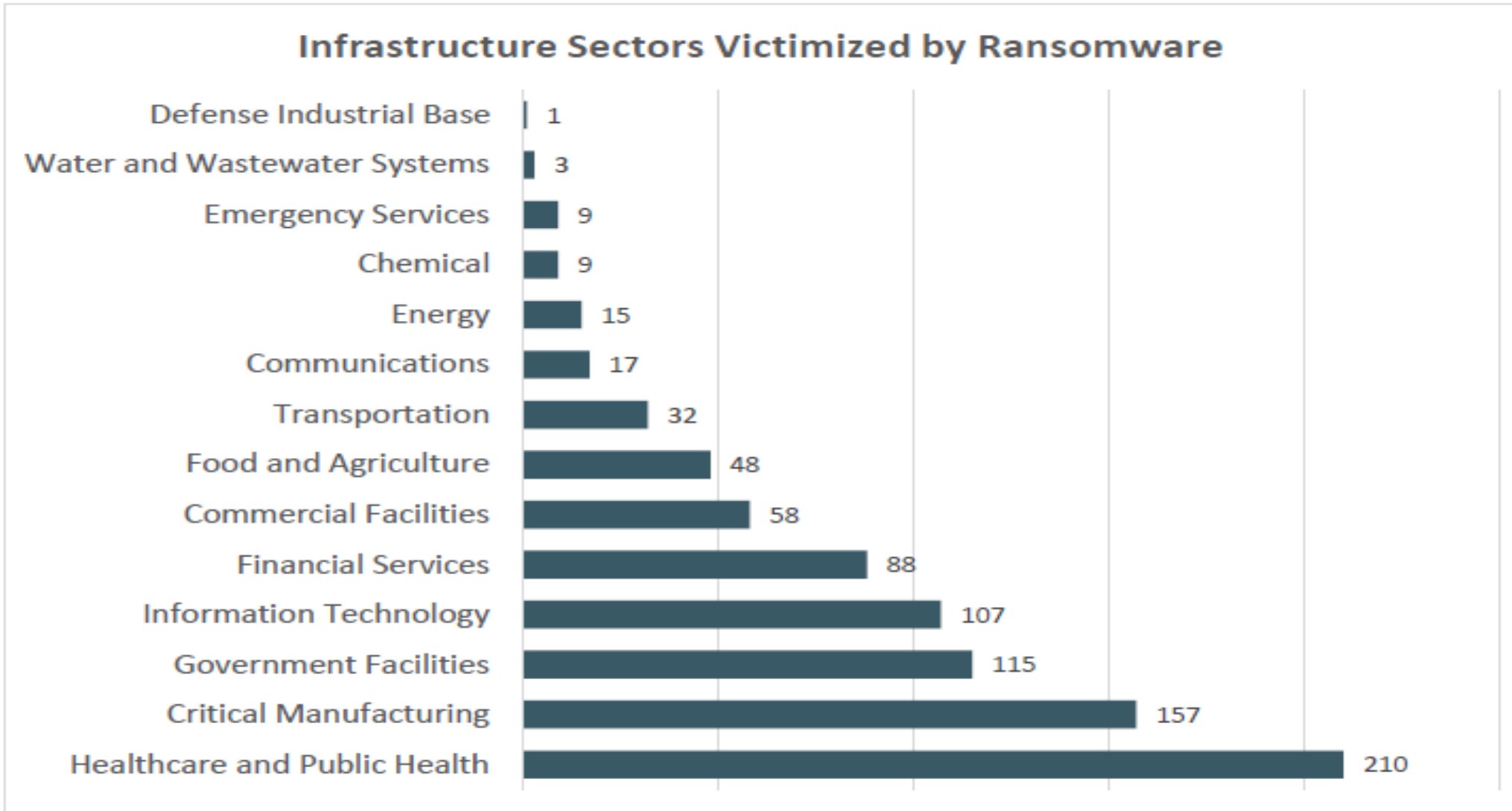


5 Year Trends – FBI Internet Crime Report 2022

Complaints and Losses over the Last Five Years*



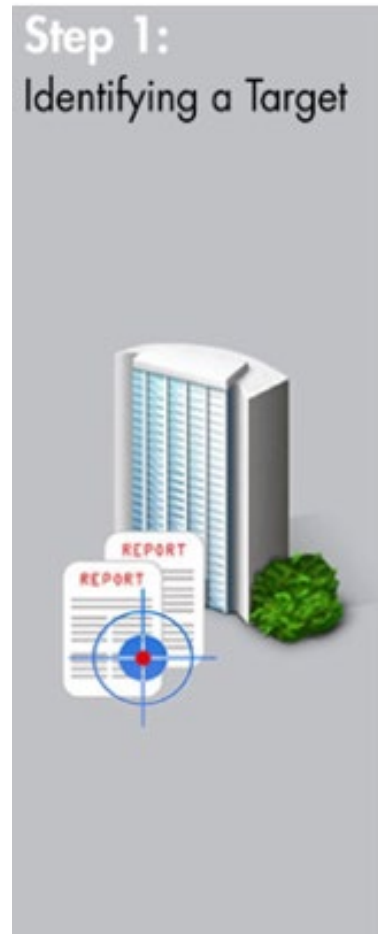
Infrastructure Sectors Hit by Ransomware



Business Email Compromise

2022 Internet Crime Complaint Center received BEC complaints with losses exceeding \$2.7B

- \$360M in calendar year 2016
- Large & small companies
- 150 countries worldwide
- Compromised email accounts
- Spoofed or Typo-squatting



Best Practices

- **Use multi-factor authentication**
- Maintain offline, encrypted backups & regularly **test**
- Create, maintain, and **exercise** a cyber incident response plan
- Conduct regular vulnerability scanning & **address vulnerabilities, especially internet-facing devices**
- Implement a **user awareness & training** program including identifying & reporting suspicious activity then **test user awareness**
- Ensure antivirus & anti-malware toolsets are **up-to-date**
- Consider risk management & cyber hygiene practices of **third parties**
- Retain & **secure logs** from both network devices and local hosts
- **Secure & monitor external services (RDP)**



These ransomware best practices and recommendations are based on operational insight from the Cybersecurity and Infrastructure Security Agency (CISA) and the Multi-State Information Sharing and Analysis Center (MS-ISAC). The audience for this guide includes information technology (IT) professionals as well as others within an organization involved in developing cyber incident response policies and procedures or coordinating cyber incident response.

Cybersecurity Performance Goals (CPGs)

- CPGs are prioritized subset of IT and OT cybersecurity practices aimed at meaningfully reducing risks to both CI operations and to the American people.
- Voluntary, Not Comprehensive, & intended to supplement the NIST CSF
- Assistance in prioritizing investment toward a limited number of high-impact security outcomes
- Enable focused improvements across suppliers, vendors, business partners, or customers
- Assist organizations impacted by, gaps in expertise, resources, & capabilities

<https://www.cisa.gov/cpg>



Outreach & Support

- **Drills & Exercises**
- **Special Event Security Planning**
- **Products:** Protective Measures, Resource Guides, Geographical Information System support, Infrastructure Visualization Platform (IVP)
- **Campaigns:** Operation Flashpoint, Elections Security, Securing Public Gatherings, School Security, Shields Up, etc.
- **Incident Support**



Training and Presentations

- CISA 101
- Active Shooter
- Bombing Threat Management
- Bombing Prevention
- Insider Threat
- Cybersecurity Awareness
- Elections Security
- Targeted Violence
- De-Escalation Training for CI
- Securing Public Gatherings
- Hometown Security
- School Security
- Security of Soft Targets and Crowded Places
- See Something, Say Something
- Counter Unmanned Aircraft Systems
- Power of Hello
- Workplace Security
- Cyber Incident Response



Exercises



Discussion-based Exercises

Seminar

Workshop

Tabletop

Operations-based Exercises

Drill

Functional

Full-Scale

Examples

- Natural Hazards
- Active Shooter
- Complex Coordinated Terrorist Attack
- Vehicle Ramming
- Improvised Explosive Device (IED)
- Phishing
- Ransomware
- Loss of Personally Identifiable Information (PII)
- Industrial Control Systems Compromise



Information Sharing

Intelligence and information sharing is essential to the protection of critical infrastructure – to enable informed decisions and timely actions:



- CISA.gov
- National Cyber Awareness System
- Homeland Security Information Network
- TRIPwire
- Information Sharing and Analysis Centers (ISACs)
- Information Sharing and Analysis Organizations (ISAOs)
- Fusion Centers
- Automated Indicator Sharing



Multi-State - Infrastructure Information Sharing & Analysis Center (MS-ISAC)

<https://www.cisecurity.org/ms-isac>

Services Included with Membership

- | | |
|---|---|
| • 24/7 Security Operation Center | • Weekly Top Malicious Domains/IP Report |
| • Incident Response Services | • Monthly Members-only Webcasts |
| • Cybersecurity Advisories and Notifications | • Access to Cybersecurity Table-top Exercises |
| • Access to Secure Portals for Communication and Document Sharing | • Vulnerability Management Program (VMP) |
| • Cyber Alert Map | • Nationwide Cyber Security Review (NCSR) |
| • Malicious Code Analysis Platform (MCAP) | • Awareness and Education Materials |



Information Sharing & Analysis Centers (ISACs)

- American Chemistry Council
- Automotive ISAC
- Aviation ISAC
- Communications ISAC
- Downstream Natural Gas ISAC
- Elections Infrastructure ISAC
- Electricity ISAC
- Emergency Management & Response ISAC
- Financial Services ISAC
- Healthcare Ready
- Health ISAC
- Information Technology ISAC
- Maritime Transportation System ISAC
- Media & Entertainment ISAC
- Multi-State ISAC
- National Defense ISAC
- Oil & Natural Gas ISAC
- Real Estate ISAC
- Research & Education Networks ISAC
- Retail & Hospitality ISAC
- Small Broadband ISAC
- Space ISAC
- Surface Transportation, Public Transportation & Over-the-Road Bus ISACS
- Water ISAC



Available Cyber Services & Tools

- Cyber Hygiene Services
- Known Exploited Vulnerabilities (KEV) Catalog
- Bad Practices Catalog
- Get Your Stuff Off Search
- No Cost Tools & Service Catalog:
 - Antivirus
 - Malware Removal
 - Investigation
 - Log analysis
 - Scanning
 - Network packet captures
 - Protocol analyzer
 - Intrusion detection & prevention
 - Threat modeling
 - Backup





Home Page | CISA
https://www.cisa.gov


- [CISA Services Catalog](#)
A single resource that provides you with access to information on services across CISA's mission areas.
- [CISA Publications](#)
Free cybersecurity tools and resources to help organizations advance their security capabilities.
- [CISA Regions](#)
CISA provides regional cyber and physical services to support security and resilience across the United States.
- [CISA Events](#)
CISA hosts and participates in events throughout the year to engage stakeholders, seek research partners, and communicate with the public to help protect the homeland.

[Return to top](#)


[Topics](#) [Spotlight](#) [Resources & Tools](#) [News & Events](#) [Careers](#) [About](#)

 **CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY**

 **CISA Central**
888-282-0870 Central@cisa.dhs.gov

 **CISA.gov**
An official website of the U.S. Department of Homeland Security

- [About CISA](#)
- [Accessibility](#)
- [Budget and Performance](#)
- [DHS.gov](#)
- [FOIA Requests](#)
- [No FFAR Act](#)
- [Office of Inspector General](#)
- [Privacy Policy](#)
- [The White House](#)
- [USA.gov](#)
- [Website Feedback](#)

 **National Terrorism Advisory System**
BULLETIN
READ MORE
[Put this widget on your web page](#)





WARREN HAGELSTIEN

Cybersecurity Advisor

Email: warren.hagelstien@cisa.dhs.gov

GREGORY GOODWATER

Protective Security Advisor

Email: gregory.goodwater@cisa.dhs.gov

