CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

SURETY ASSOCIATION OF SOUTH TEXAS

TRAVELERS LUNCH AND LEARN

Todd Vasilou
Cybersecurity Advisor
CISA Region 6

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

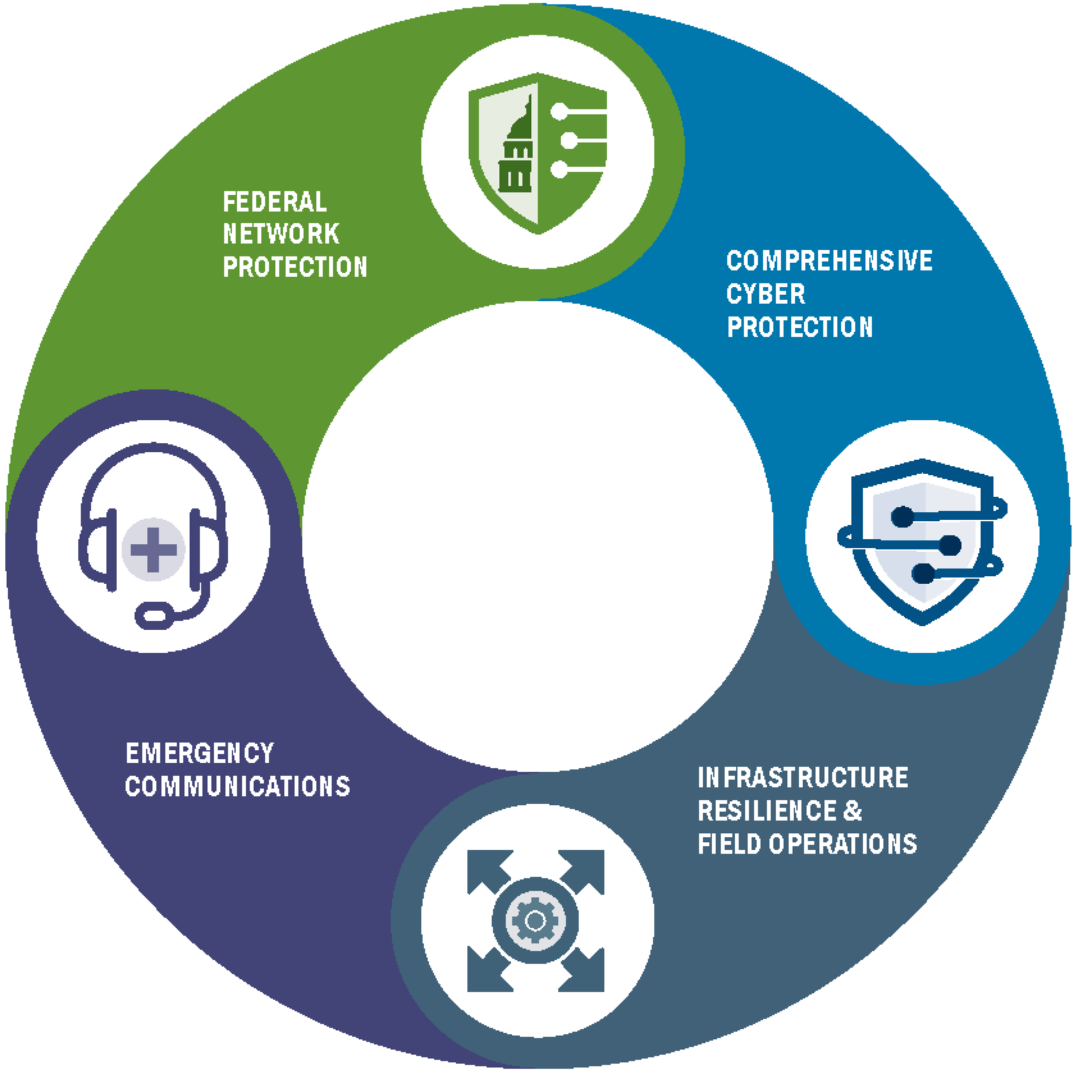
Strengthen critical infrastructure and address long-term risks

months | years | decades

CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY

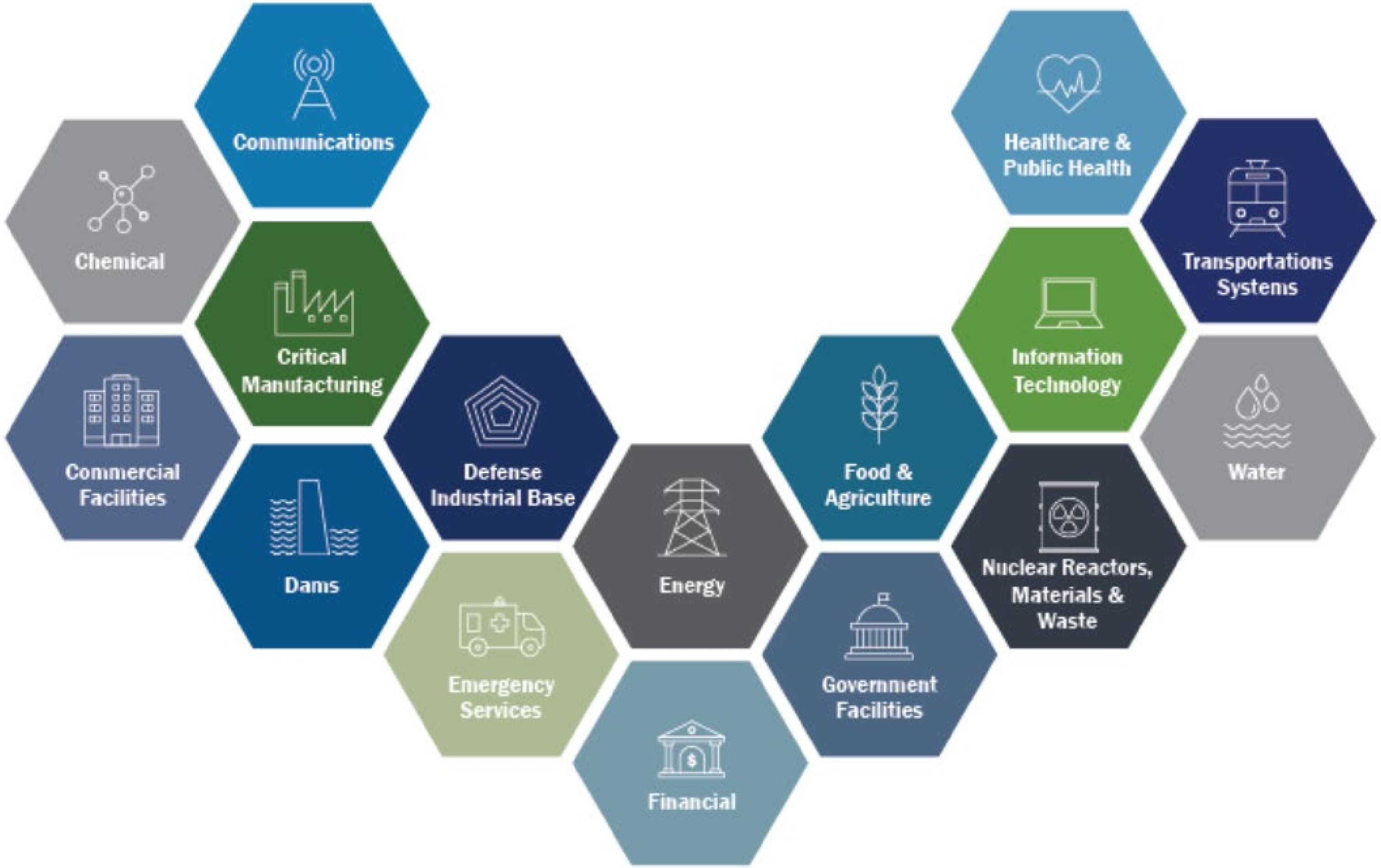
We are the Nation's Risk Advisor

The Cybersecurity and Infrastructure Security Agency (CISA) is the pinnacle of national risk management for cyber and physical infrastructure


FEDERAL NETWORK PROTECTION
COMPREHENSIVE CYBER PROTECTION
INFRASTRUCTURE RESILIENCE & FIELD OPERATIONS
EMERGENCY COMMUNICATIONS

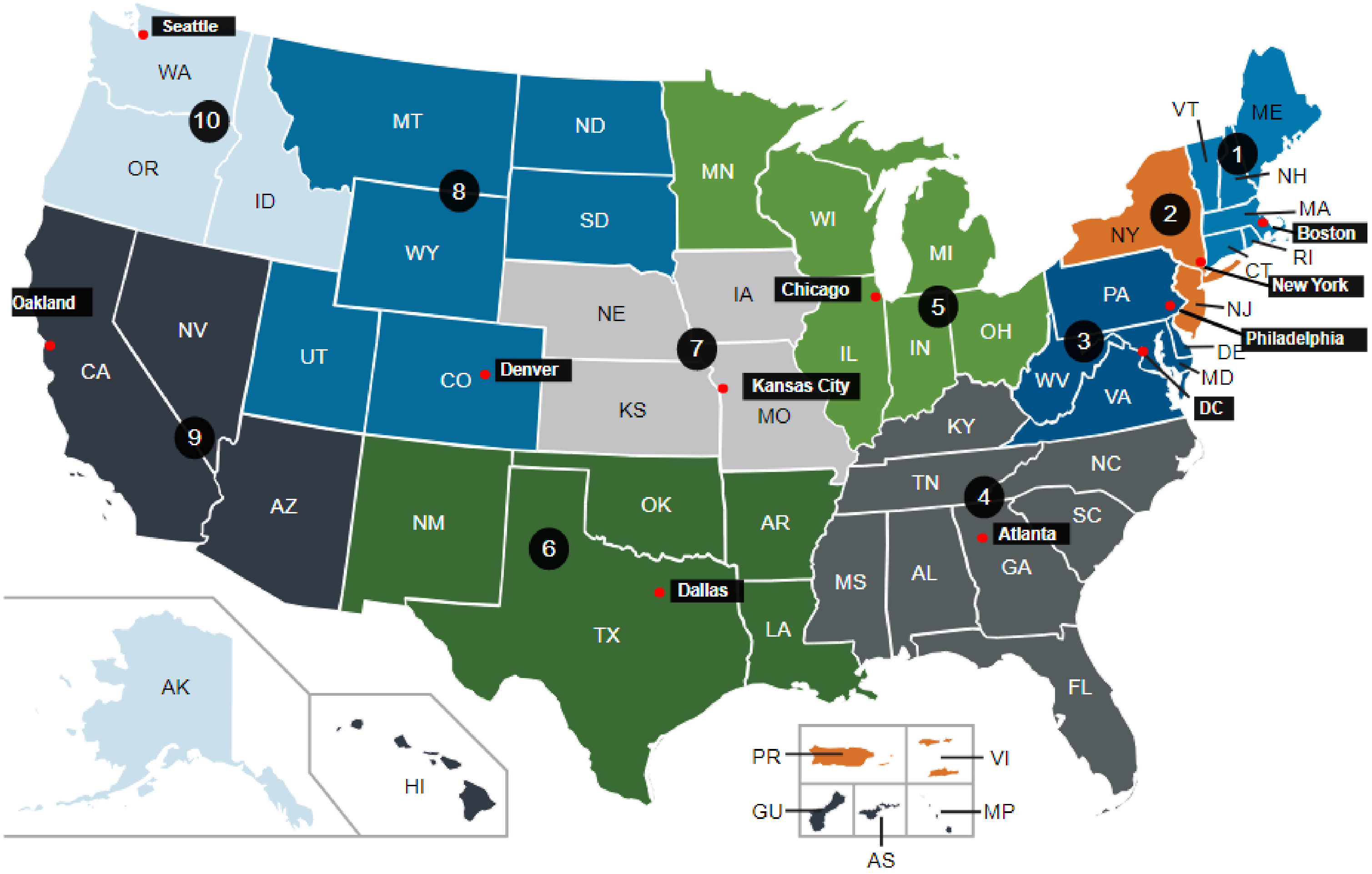
Critical Infrastructure Sectors

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



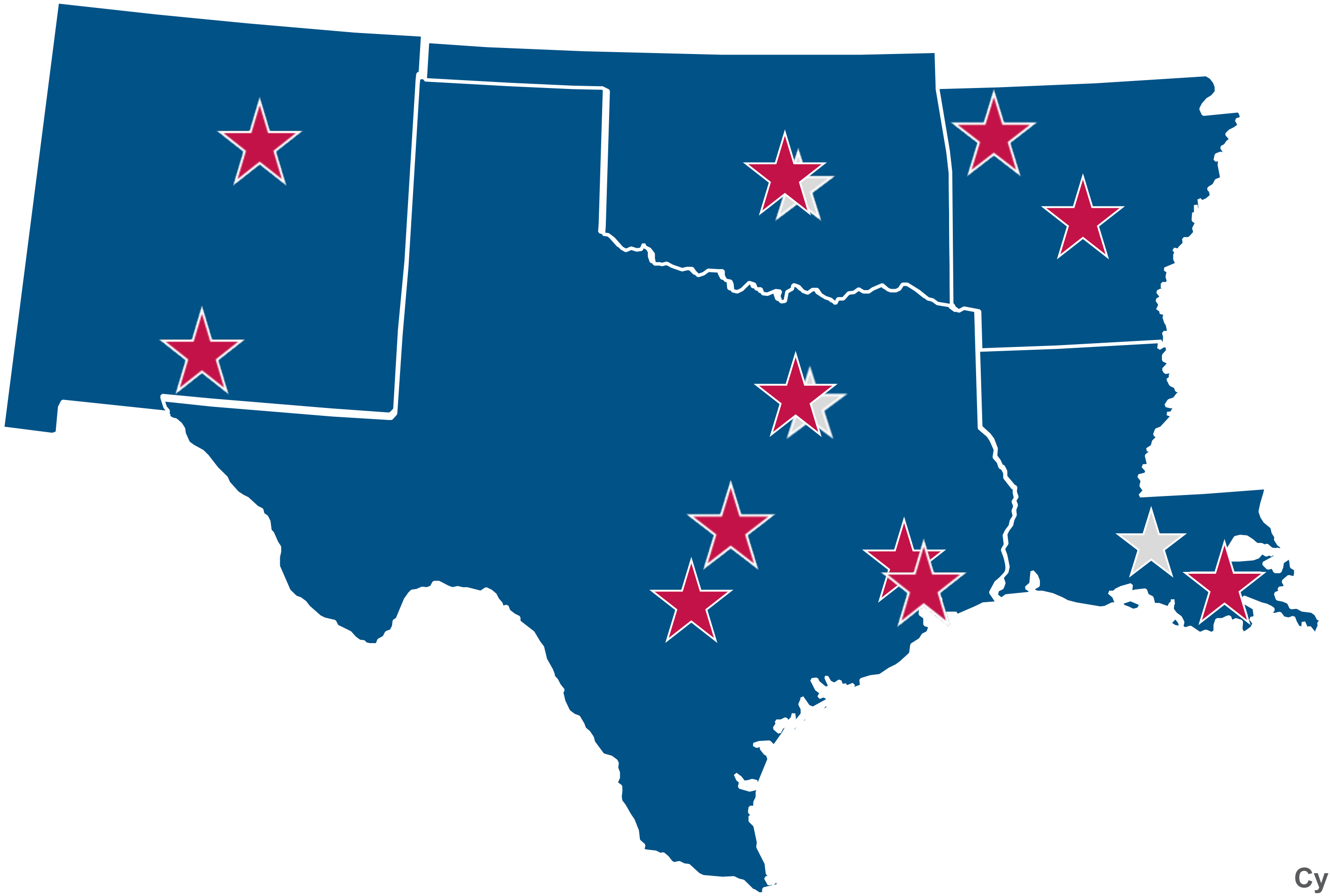
CISA Region 6: CISARegion6@hq.dhs.gov

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.

Reg 6 | On-Hand / Projected Cyber Personnel



★ On-Hand

☆ Projected

CISA THREAT BRIEFING

THREAT LANDSCAPE AND FOUNDATIONAL CONCEPTS

What is cybersecurity?

Definition: Cybersecurity

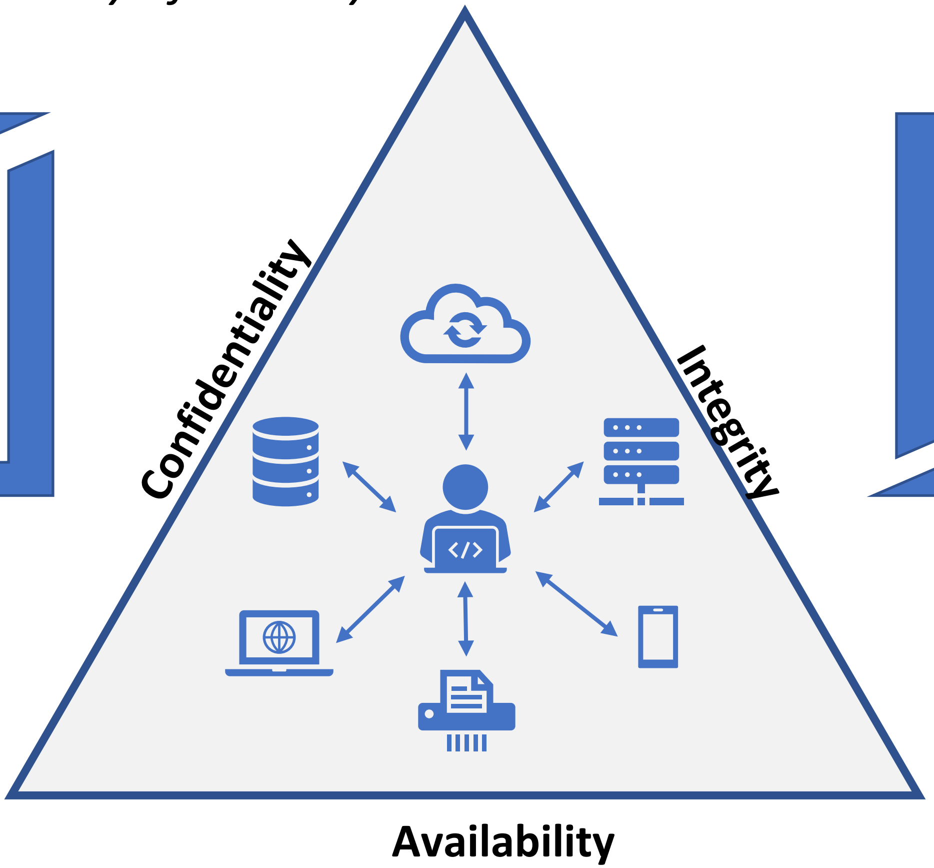
According to NIST, cybersecurity is *"the prevention of damage to, unauthorized use of, exploitation of, and—if needed—the restoration of electronic information and communications systems, and the information they contain, in order to strengthen the confidentiality, integrity and availability of these systems."*

National Institute of Standards and Technology

Source: NIST Glossary of Terms

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

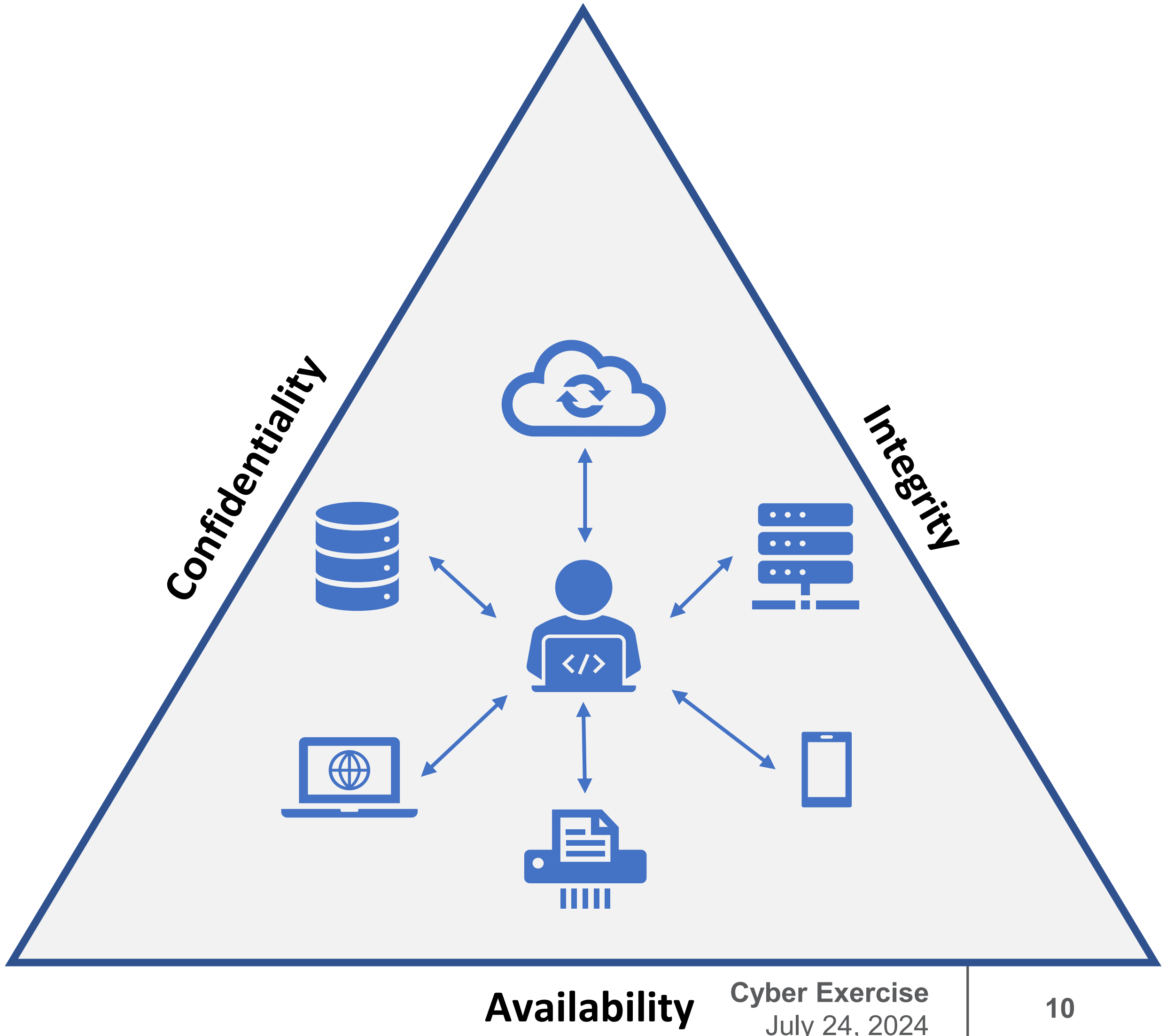
Core Principles of Cybersecurity

C Prevent unauthorized access and use of information resources

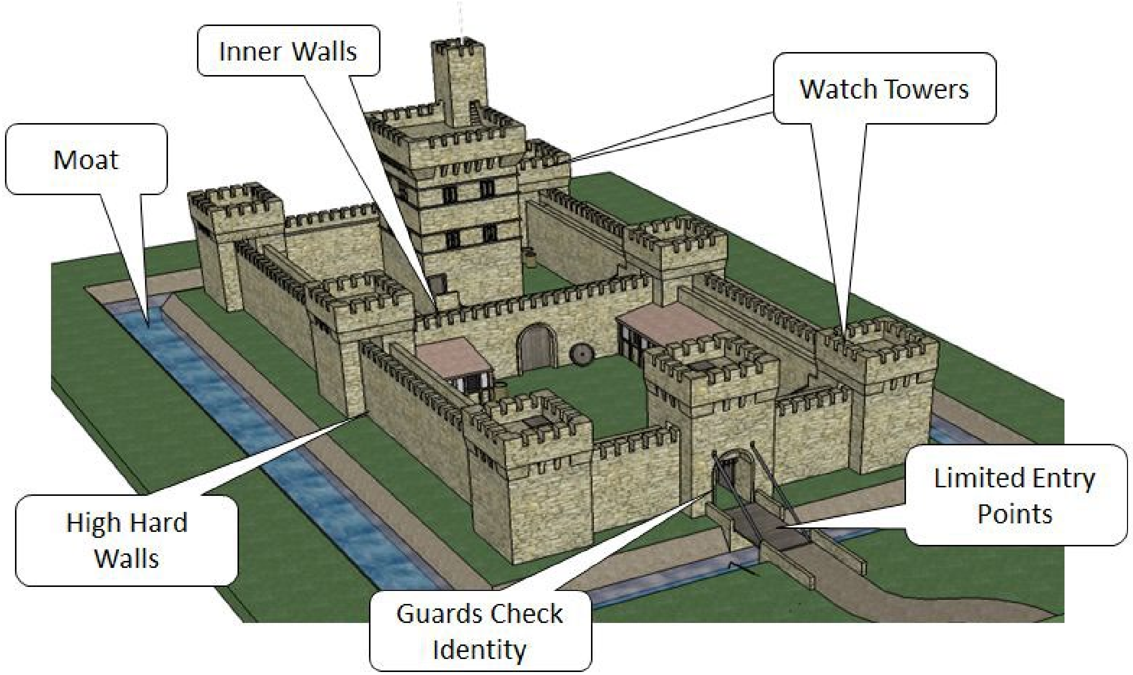
I Prevent unauthorized change and ensure reliability of information resources

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.

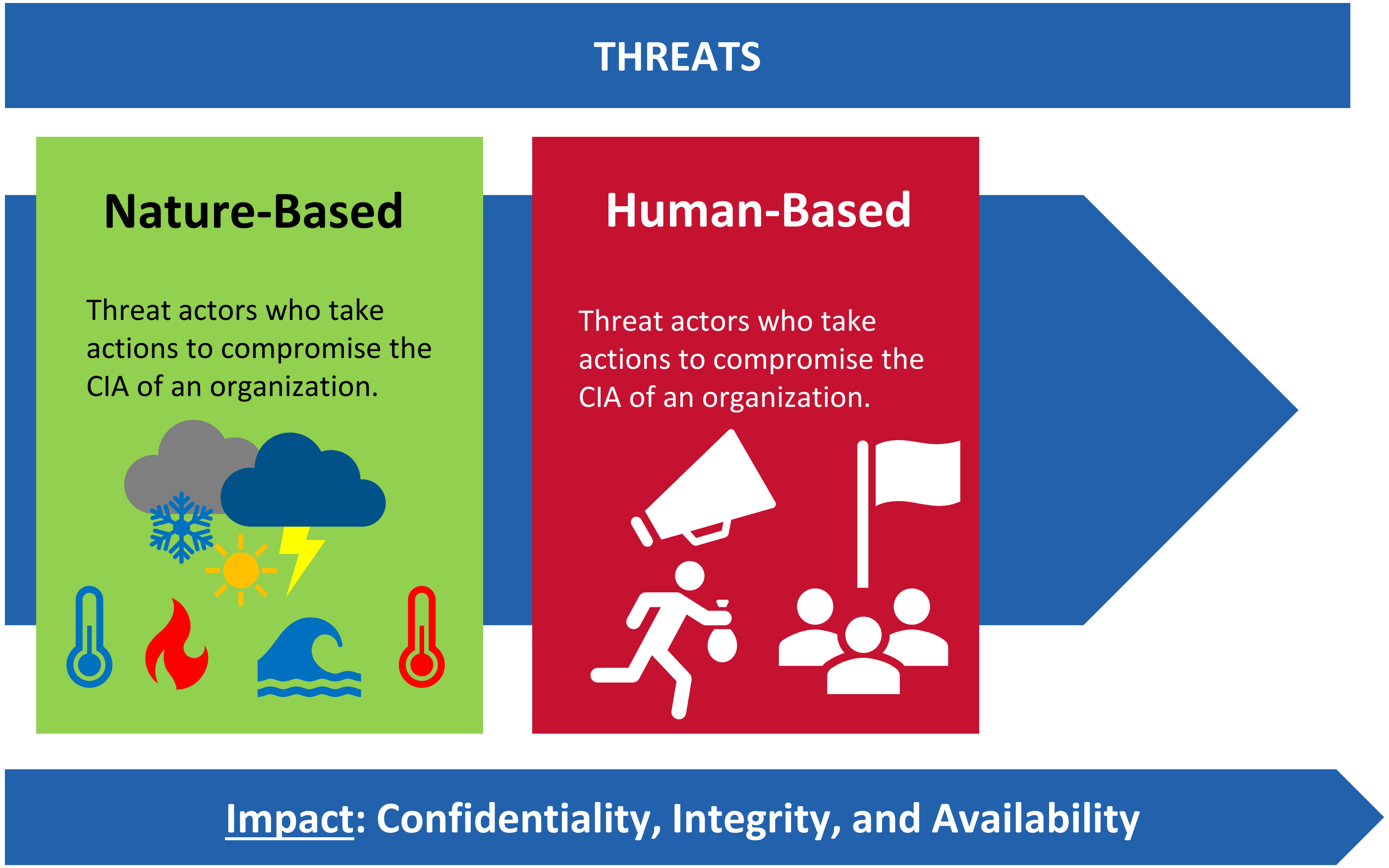


What are you trying to protect?



- Customer Data
- IT Assets and network Infrastructure
- Intellectual Property
- Finances and Financial Data
- Service Availability and Productivity
- Reputation and Trust

Threats



THREATS

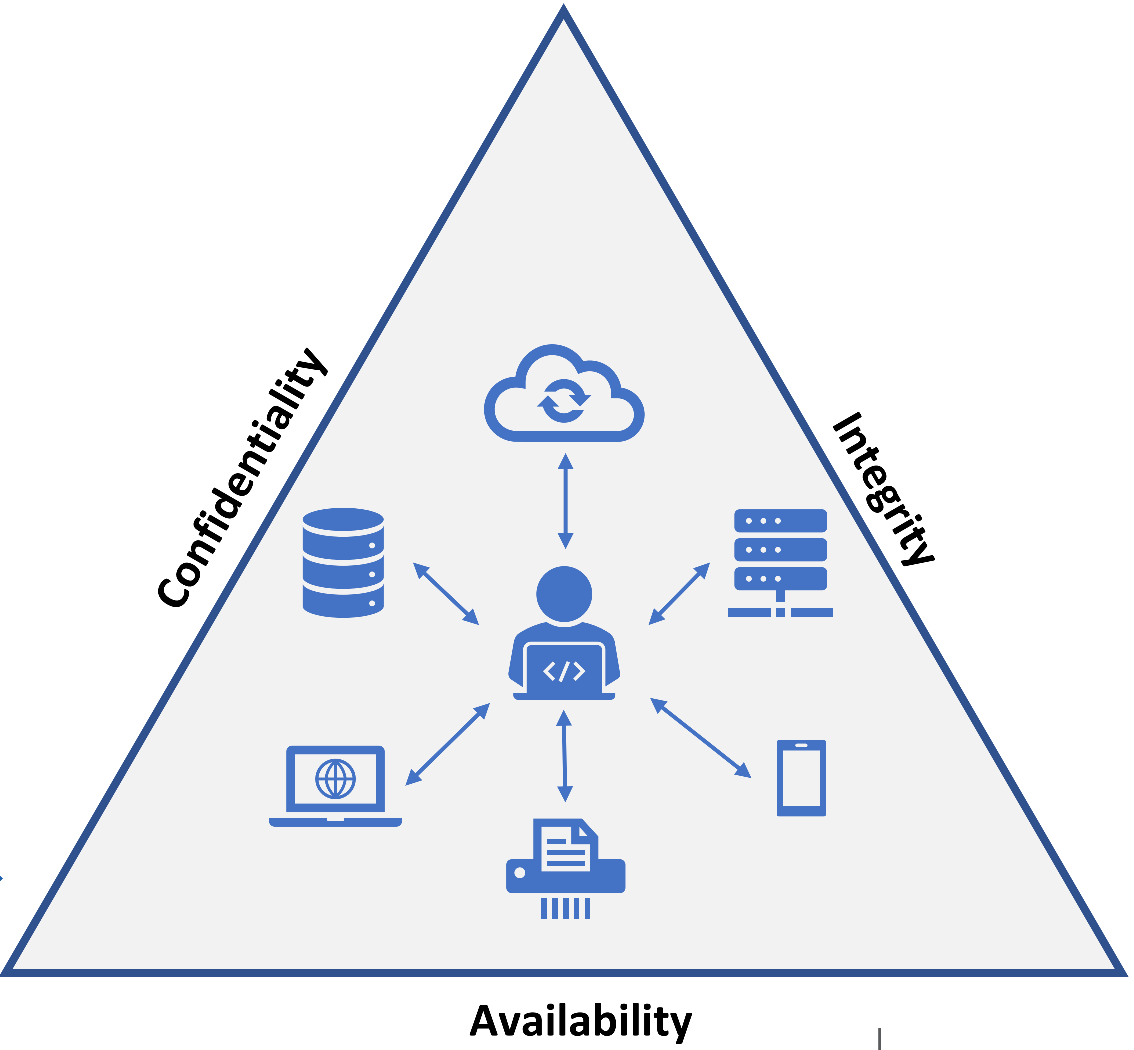
Nature-Based

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

Human-Based

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

Impact: Confidentiality, Integrity, and Availability



Threat Actors

THREAT ACTORS

HACKTIVISTS

Conduct attacks in furtherance of political interests.

CRIMINALS

Conduct attacks in furtherance of financial interests.

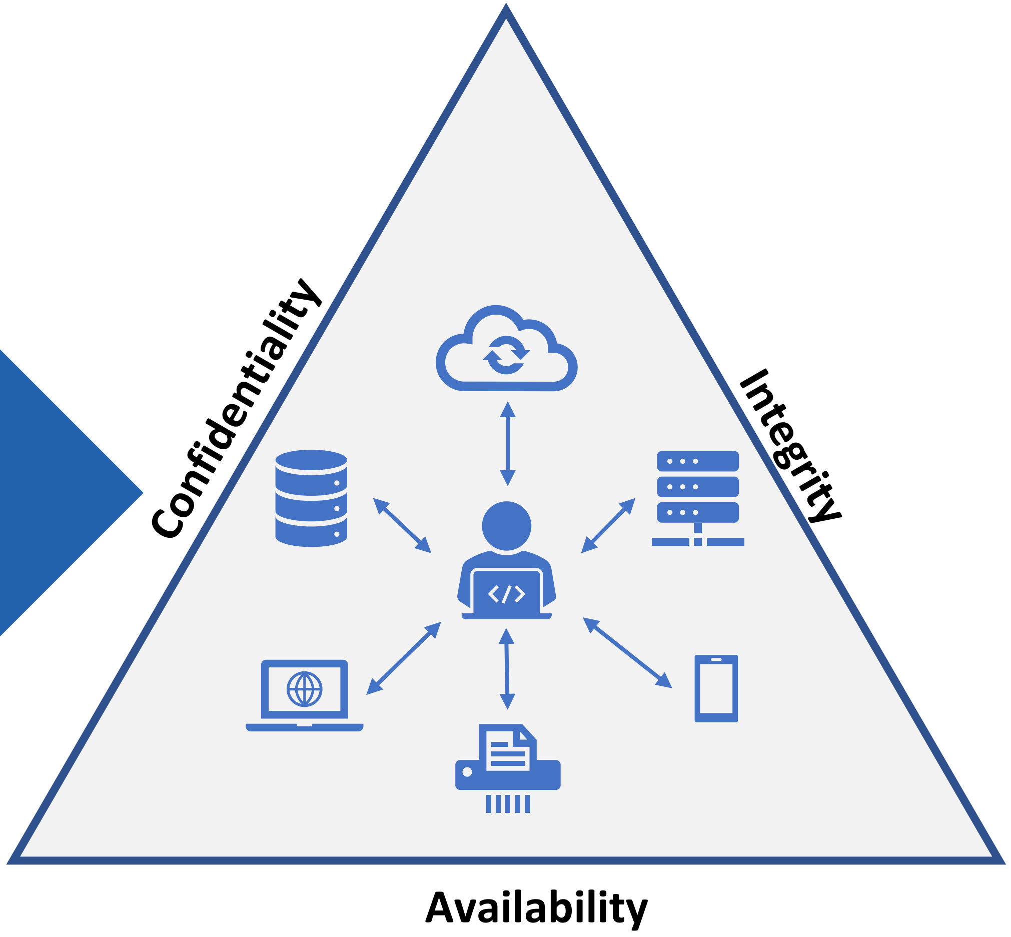
INSIDERS

Conduct attacks in furtherance of personal interests.

STATE ACTORS

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

Impact: Confidentiality, Integrity, and Availability

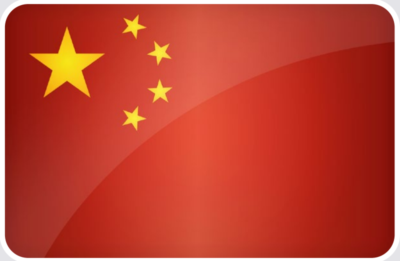


ODNI 2022 Annual Threat Assessment

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.

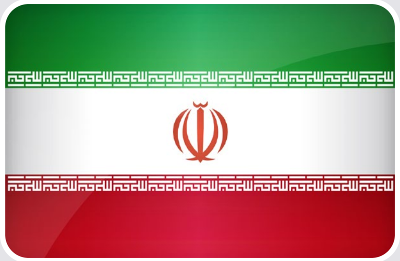
- Considers cyber attacks an acceptable option to deter adversaries, control escalation, and prosecute conflicts.



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.

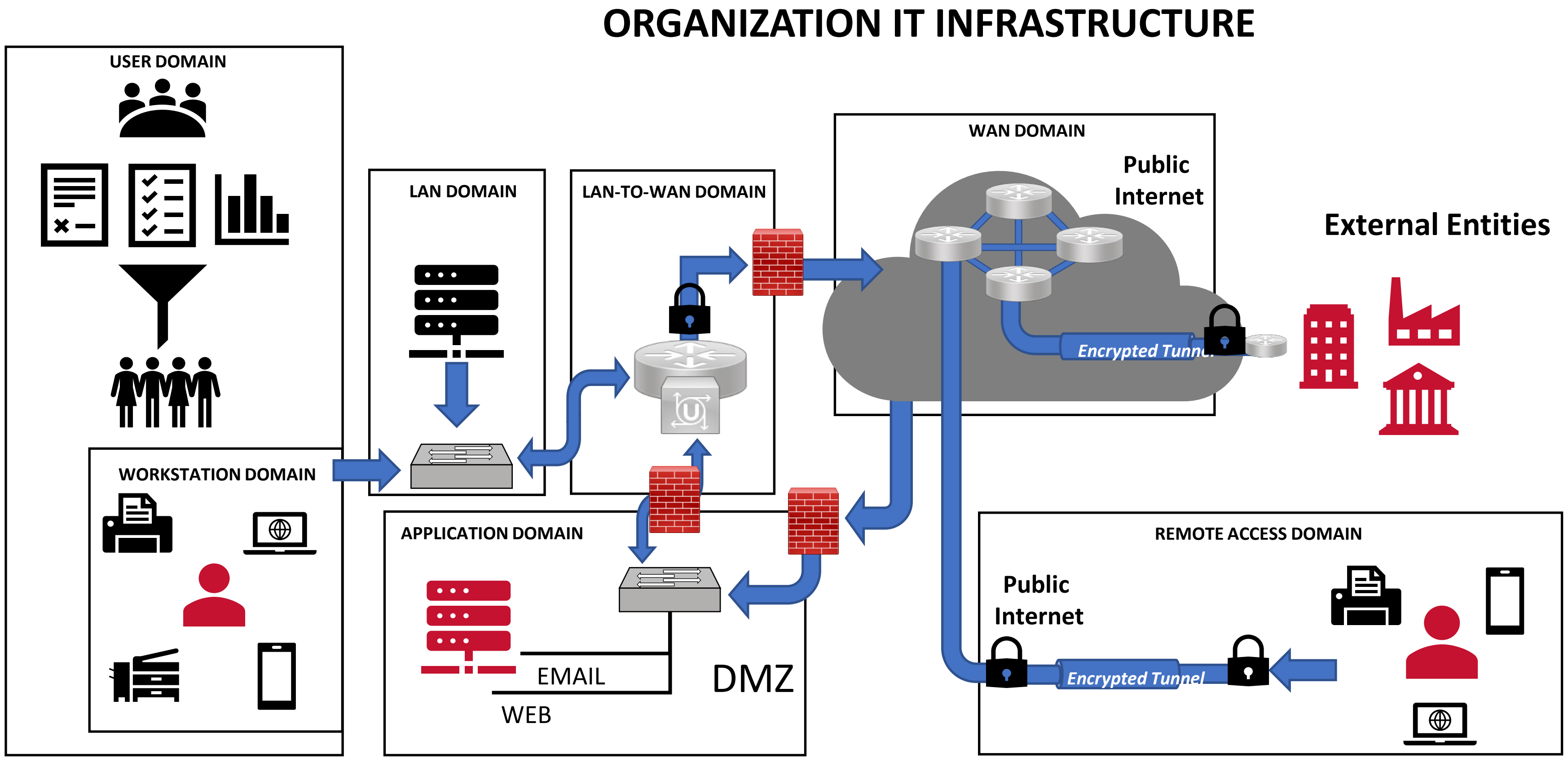
- Responsible for multiple cyber attacks against Israeli water facilities.

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



THREAT ACTORS

Planning
- Identify target(s)

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

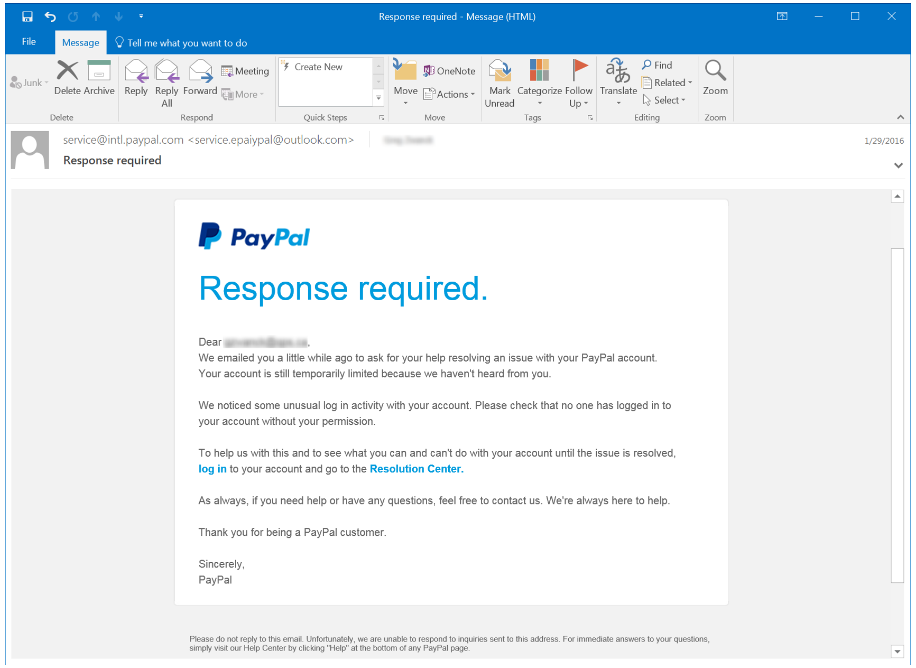
Attack
- Gain access
- Maintain access
- Hide tracks
- Accomplish attack goal

Prime Targets: Vulnerable Users, Technology, and External Partners/Vendors

Social Engineering Attacks: Attacks on Vulnerable 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)



service@intl.paypal.com <service.epaiypal@outlook.com> [redacted] 1/29/2016

Response required

PayPal

Response required.

Dear [redacted],
We emailed you a little while ago to ask for your help resolving an issue with your PayPal account. Your account is still temporarily limited because we haven't heard from you.

We noticed some unusual log in activity with your account. Please check that no one has logged in to your account without your permission.

To help us with this and to see what you can and can't do with your account until the issue is resolved, **log in** to your account and go to the **Resolution Center.**

As always, if you need help or have any questions, feel free to contact us. We're always here to help.

Thank you for being a PayPal customer.

Sincerely,
PayPal

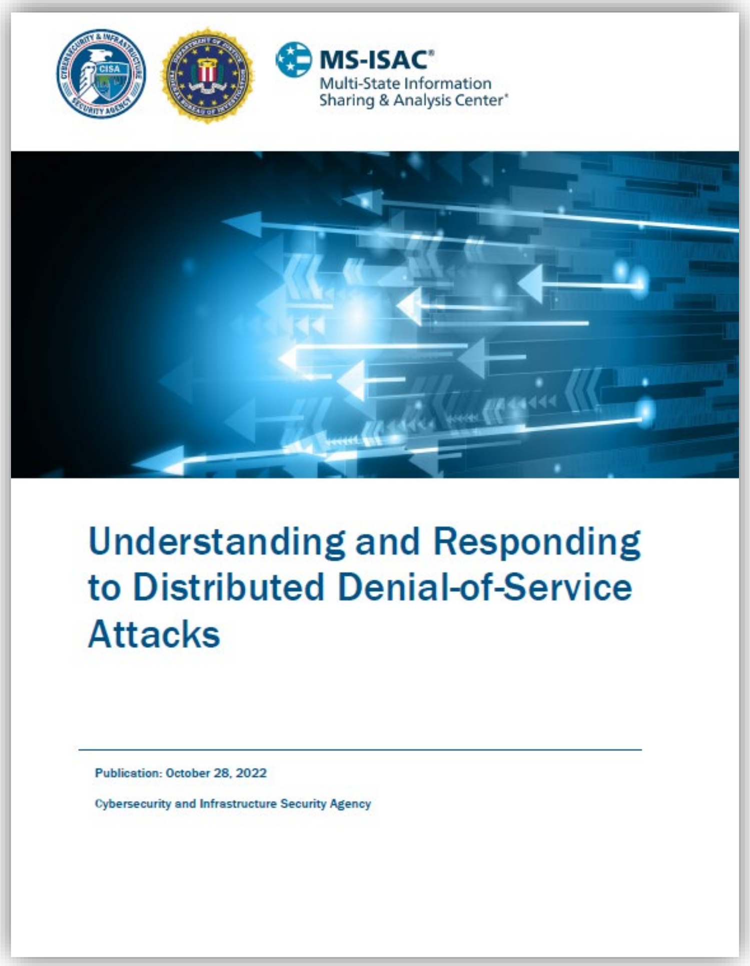
Please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking "Help" at the bottom of any PayPal page.

Image Source: knowbe4.com

Denial of Service Attacks: Attacks on Vulnerable Technology

Denial of Service Attacks

- **Description**:
  - According to CISA, **Denial of Service Attack** refers to *"[a] type of cyberattack targeting a specific application or website with the goal of exhausting the target system's resources, which, in turn, renders the target unreachable or inaccessible, denying legitimate users access to the service."* **Source***:* Understanding and Responding to Distributed Denial of Service Attacks (CISA)
- **Threat Actor Objective**:
  - To deny legitimate access to and use of system resources.
  - Often used as a distraction.
- **Common Threat Actor Techniques**:
  - Network resource overload
  - Protocol resource overload
  - Application resource overload



MS-ISAC®
Multi-State Information
Sharing & Analysis Center®

Understanding and Responding to Distributed Denial-of-Service Attacks

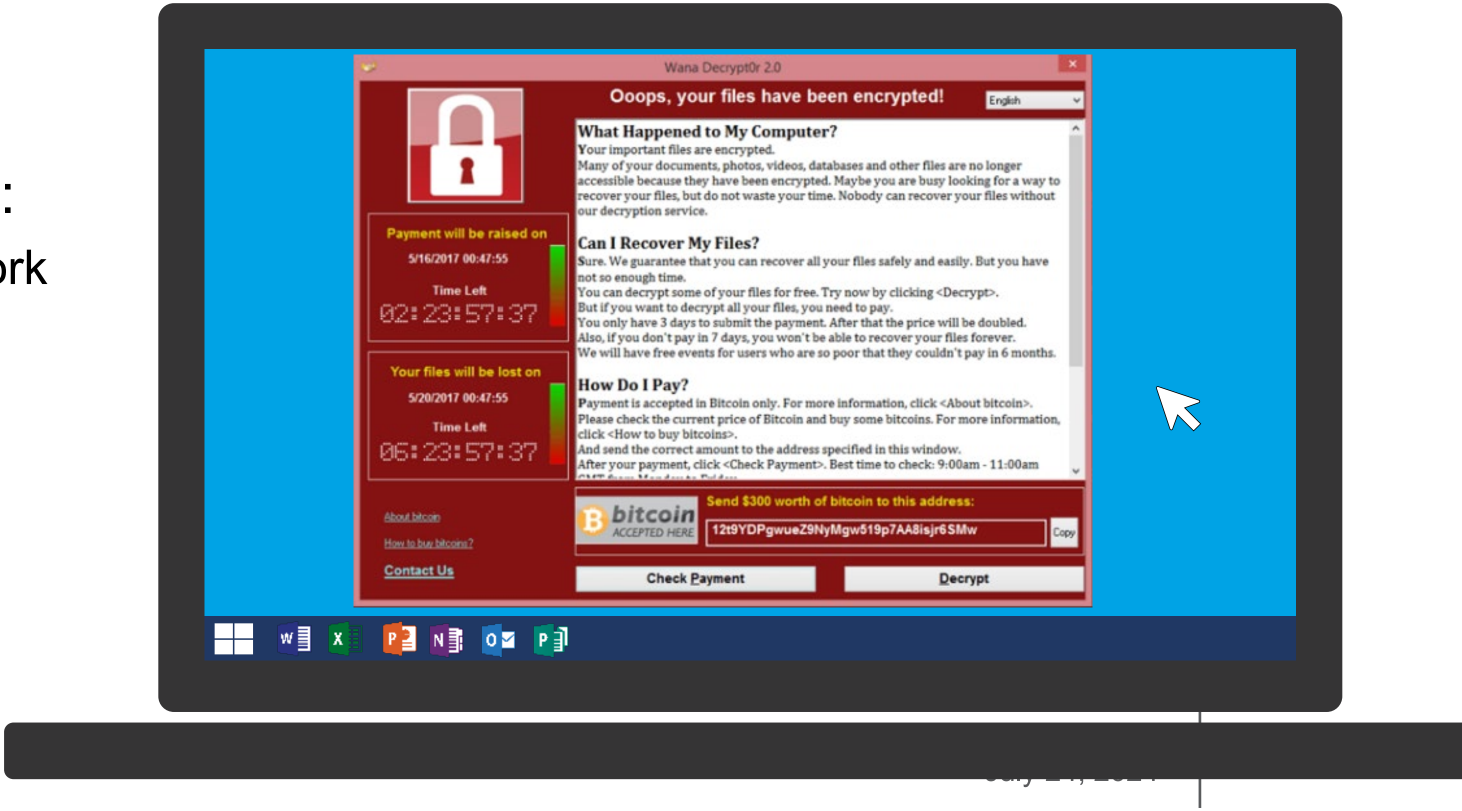
Publication: October 28, 2022

Cybersecurity and Infrastructure Security Agency

Ransomware Attacks: Attacks on Vulnerable Technology

Ransomware Attack

- **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
- **Threat Actor Objective**:
  - Hold your data for ransom
- **Common Threat Actor Techniques**:
  - Gain unauthorized access to your network
    - Compromise vulnerable users
    - Compromise vulnerable systems
  - Compromise accounts
  - Establish a foothold in your network
  - Encrypt your data and execute ransom



Wana Decrypt0r 2.0

Ooops, your files have been encrypted!

English

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

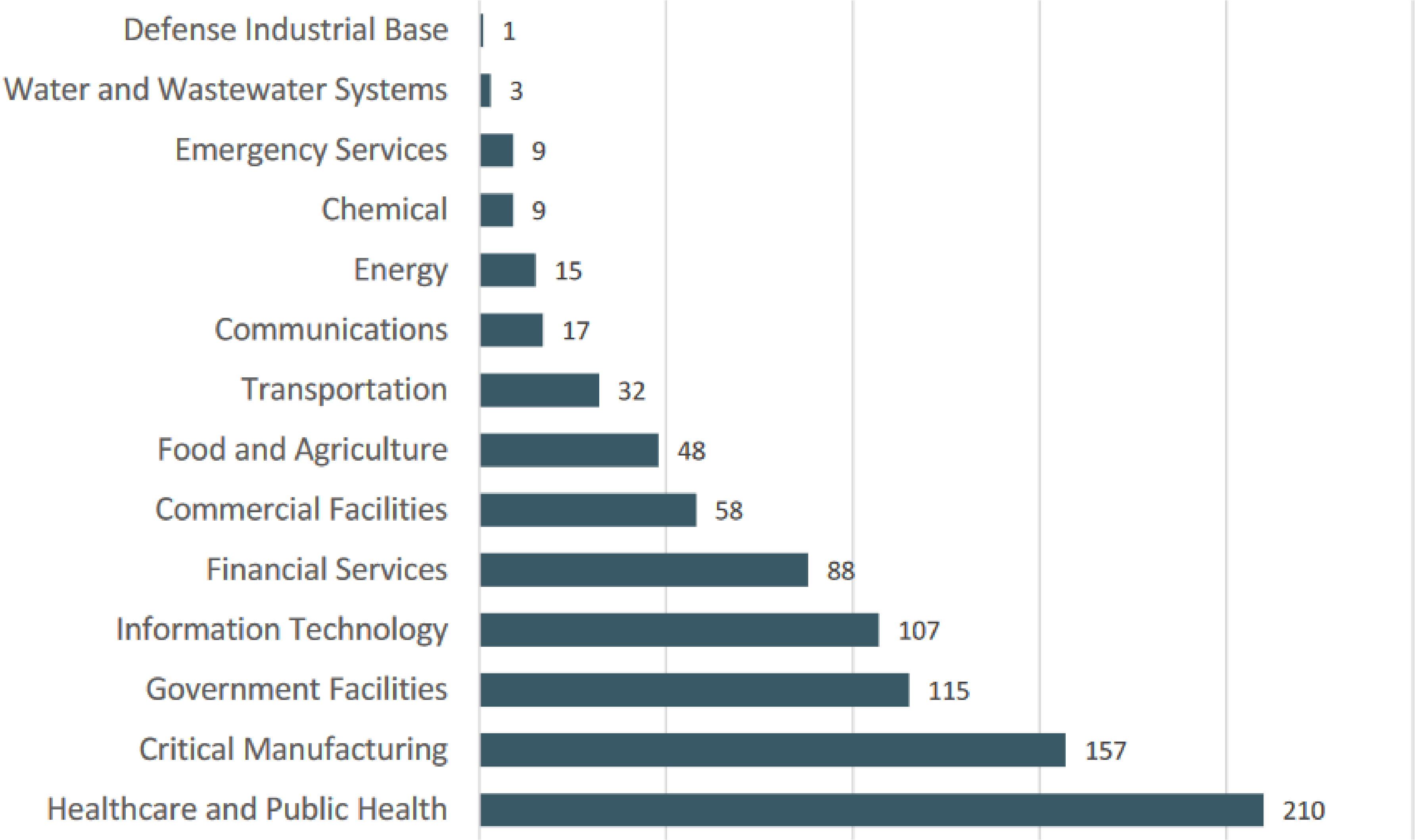
Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

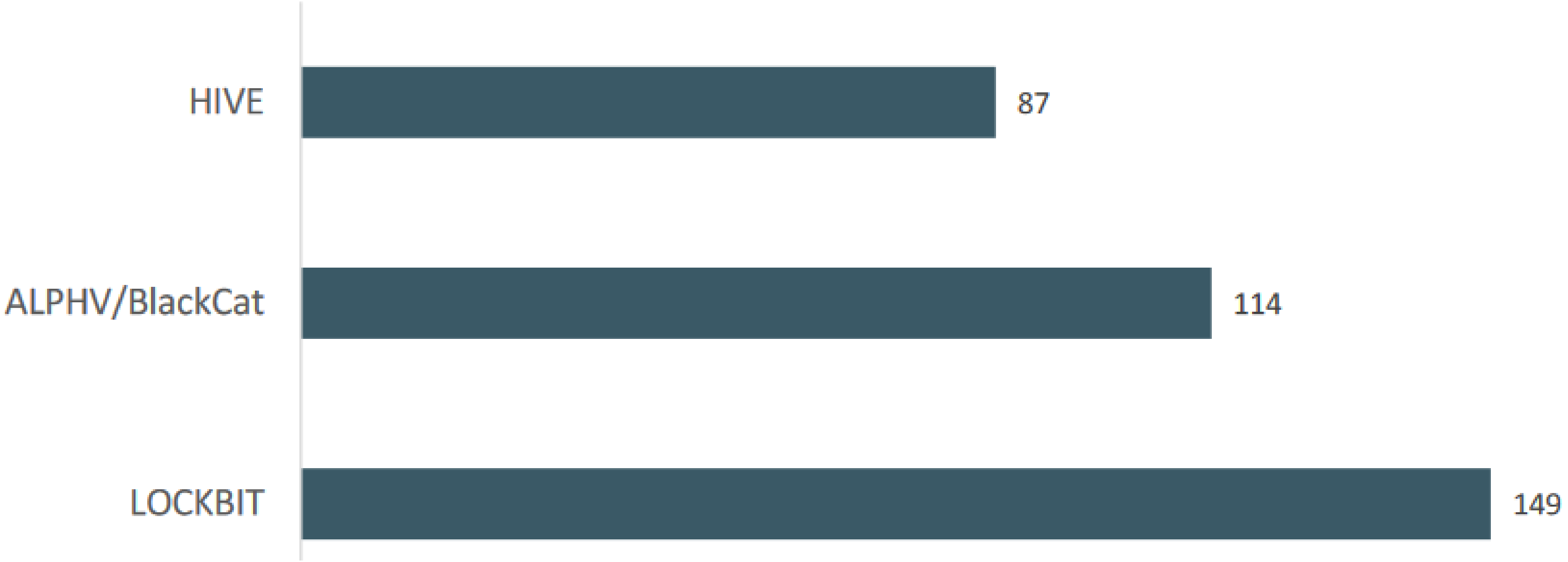
TEXAS

Infrastructure Sectors Victimized by Ransomware



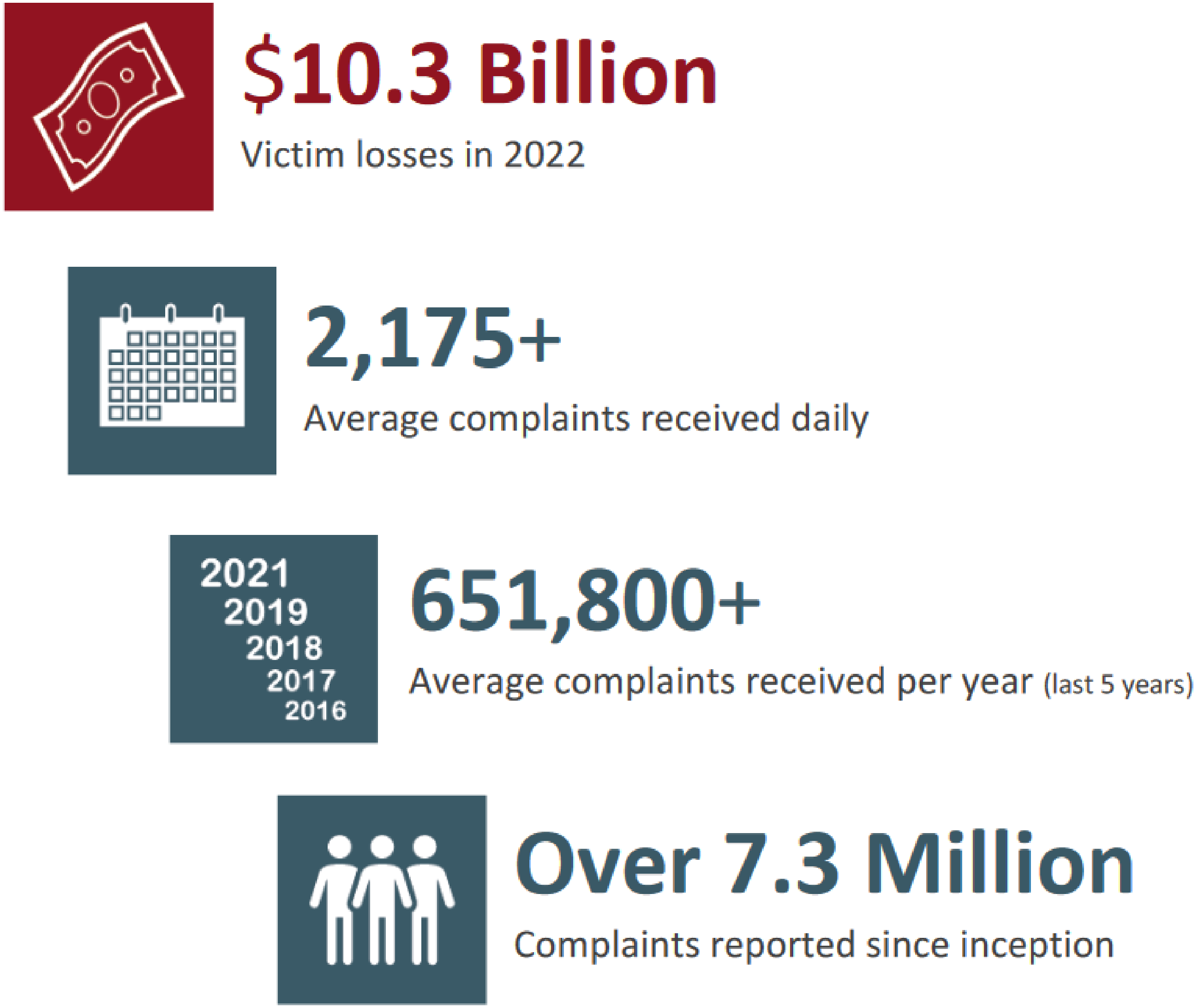
Source FBI IC3 2022 Annual Report

Top Ransomware Variants 2022 Incidents



Source FBI IC3 2022 Annual Report

2022 Statistics



$10.3 Billion

Victim losses in 2022

2,175+

Average complaints received daily

2021
2019
2018
2017
2016

651,800+

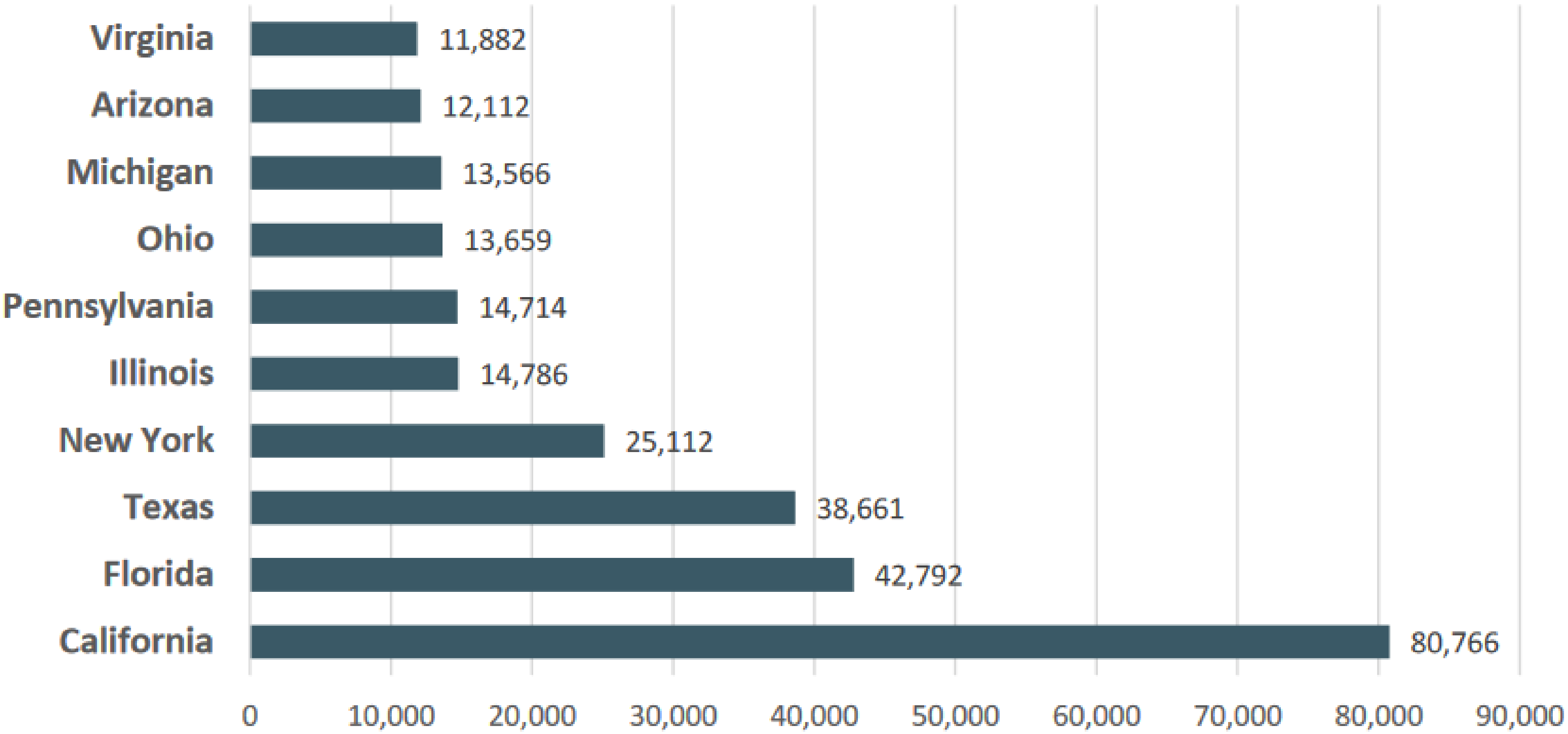
Average complaints received per year (last 5 years)

Over 7.3 Million

Complaints reported since inception

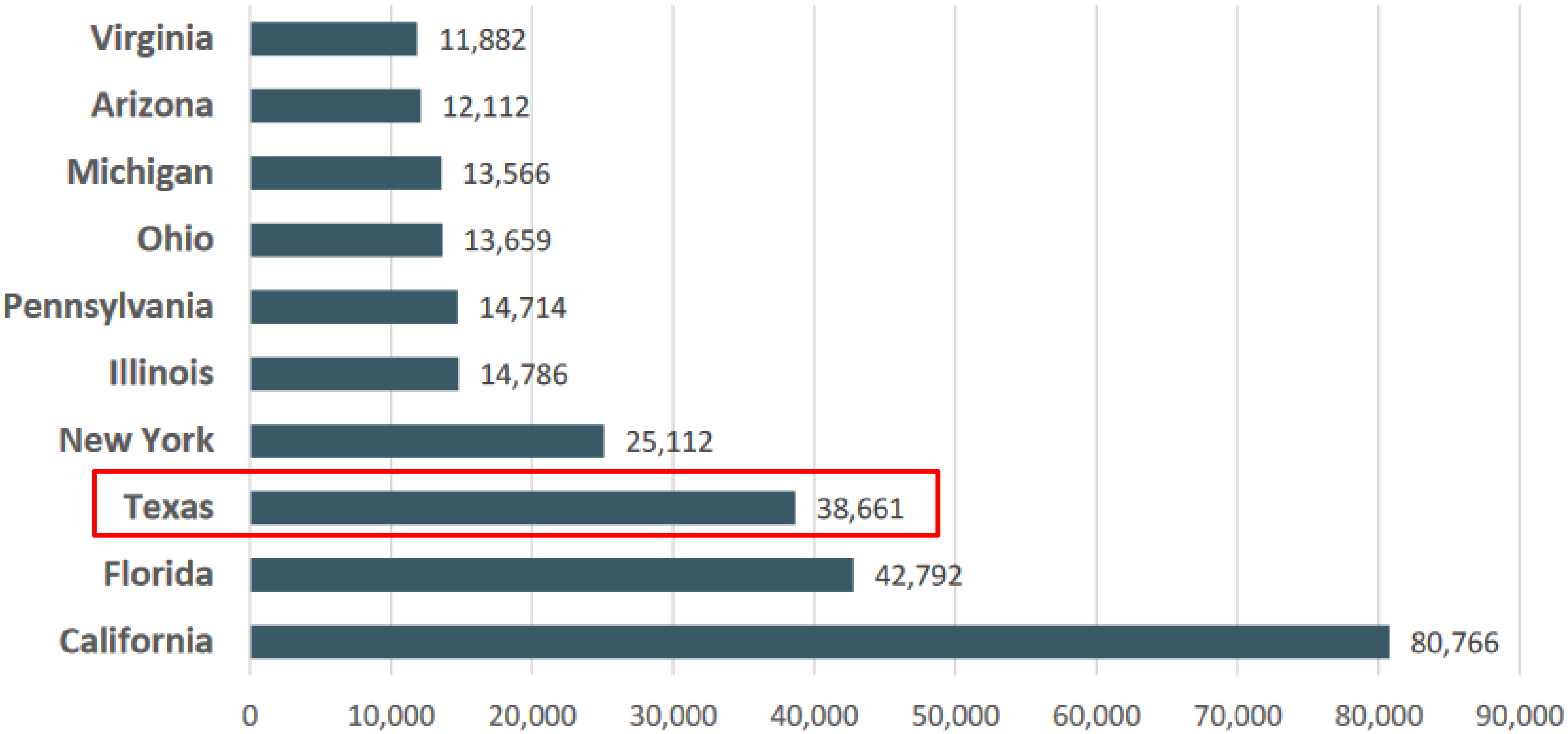
Source FBI IC3 2022 Annual Report

2022 – Top 10 States by Number of Victims



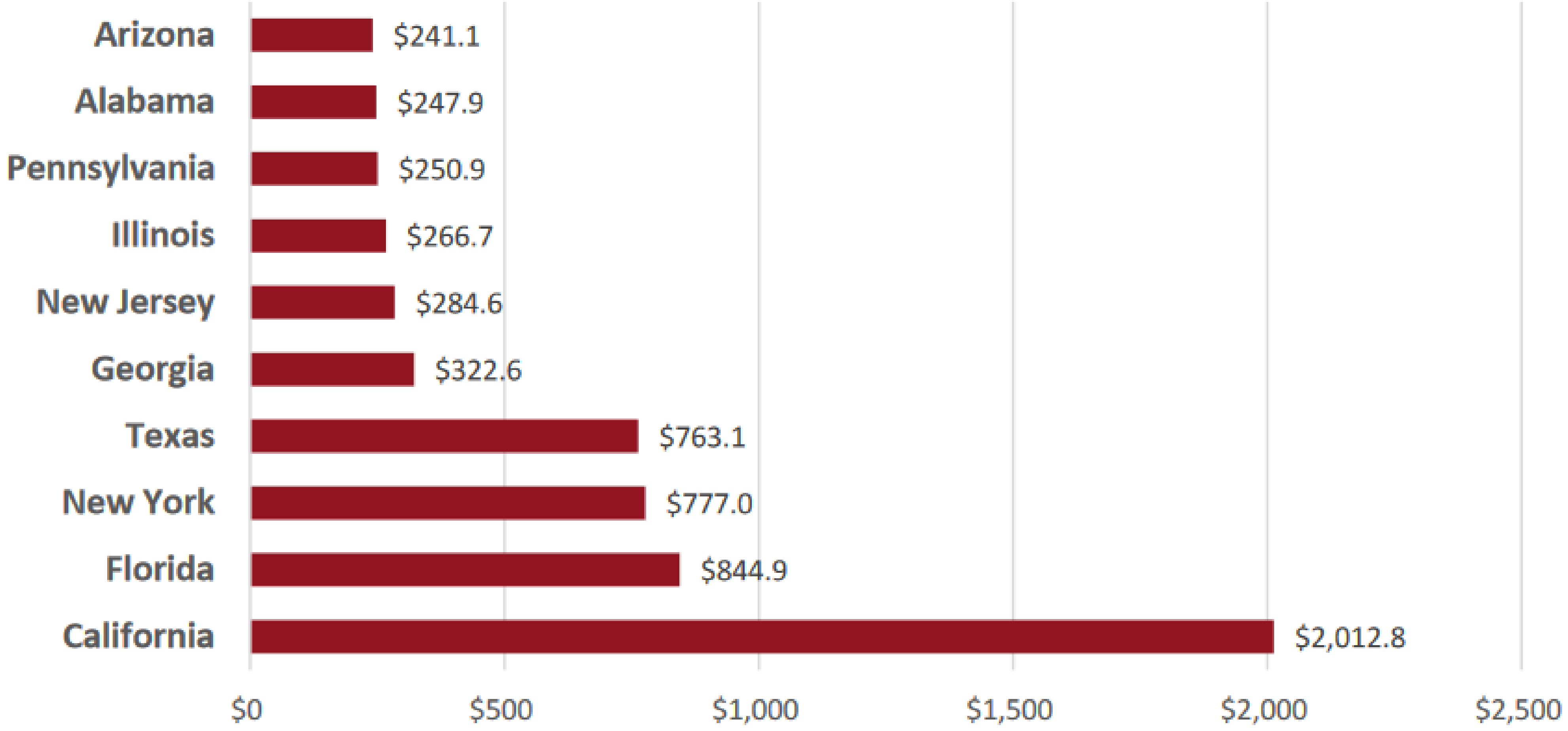
Source FBI IC3 2022 Annual Report

2022 – Top 10 States by Number of Victims



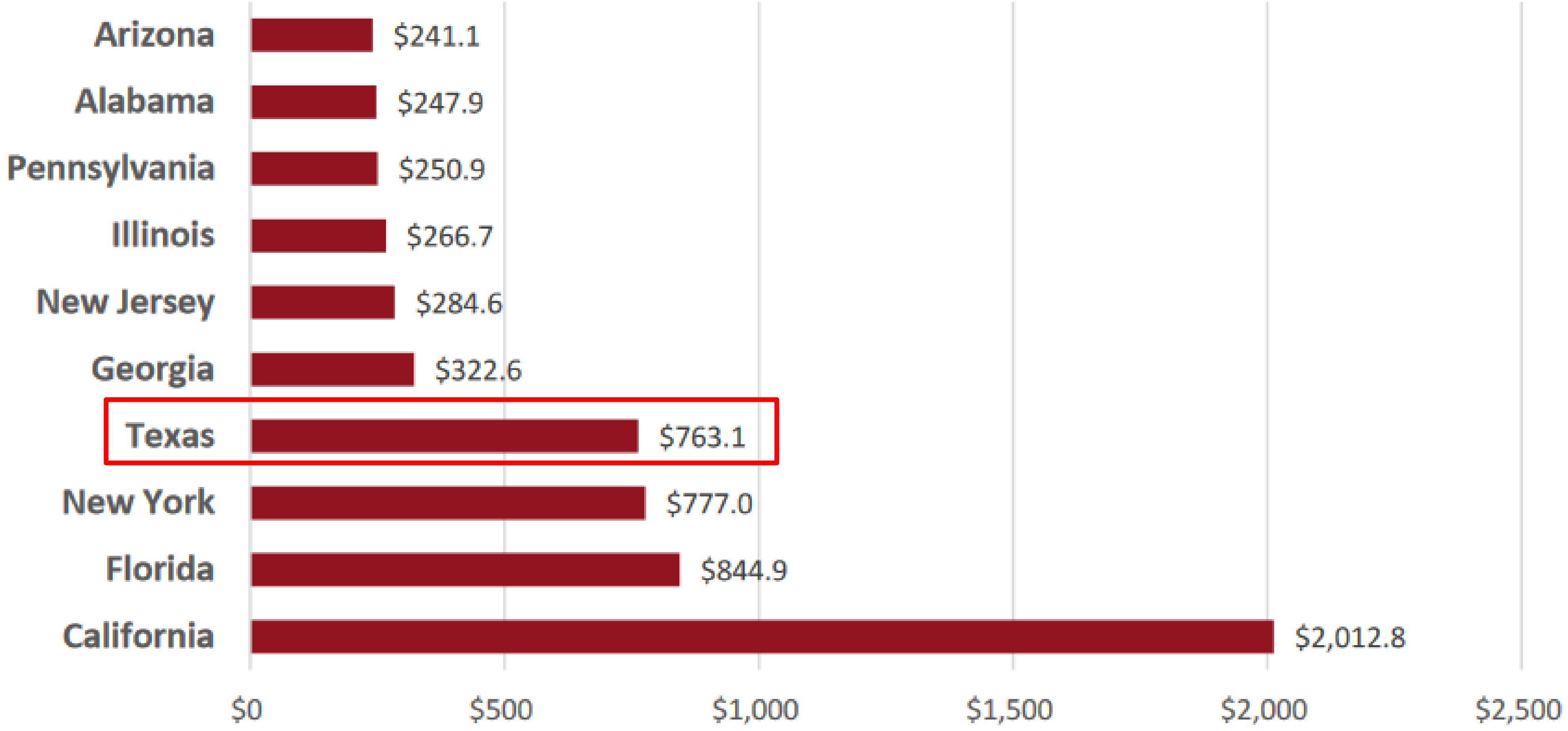
Source FBI IC3 2022 Annual Report

2022 – Top 10 States by Victim Loss (in Millions)



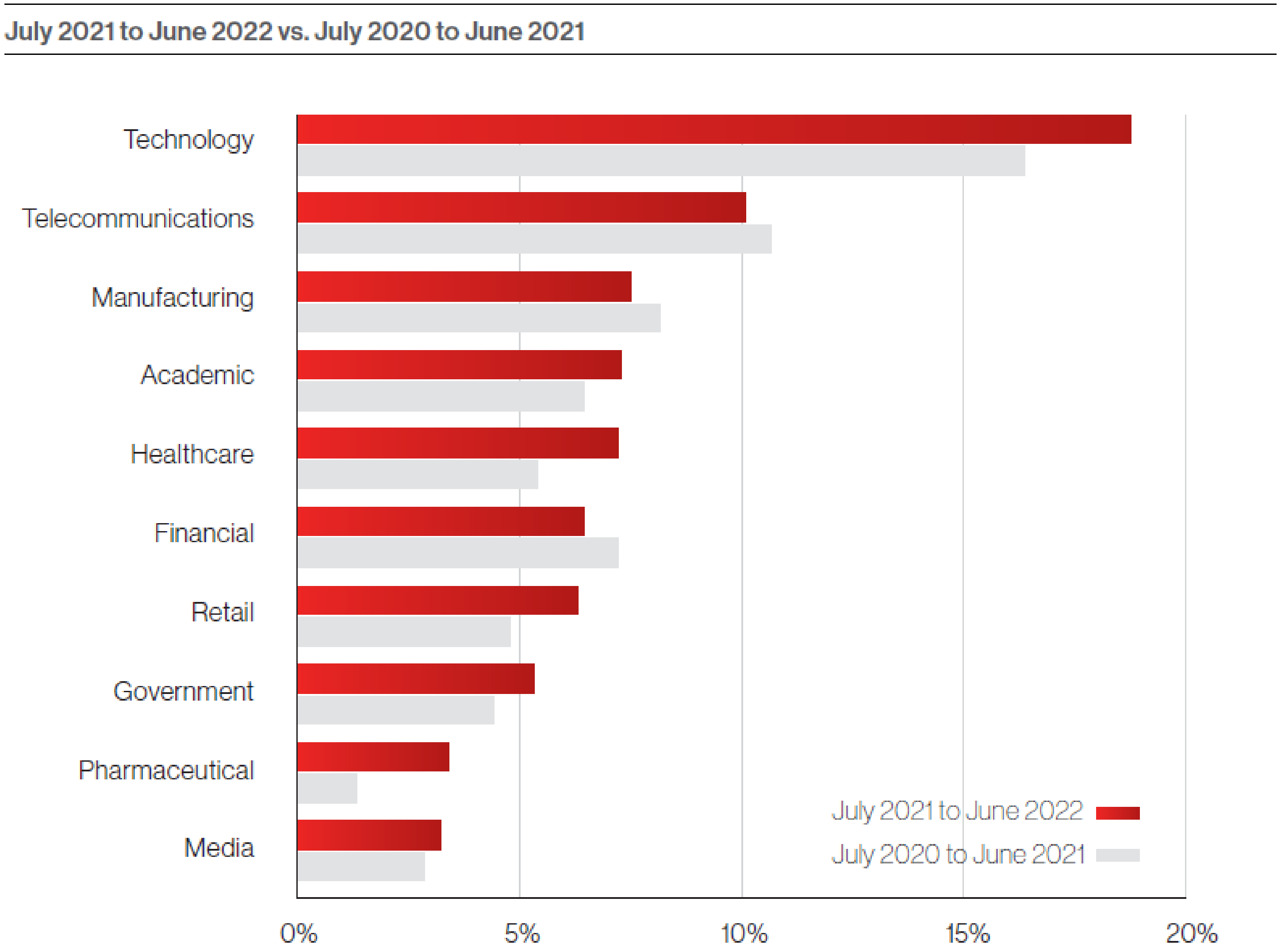
Source FBI IC3 2022 Annual Report

2022 – Top 10 States by Victim Loss (in Millions)



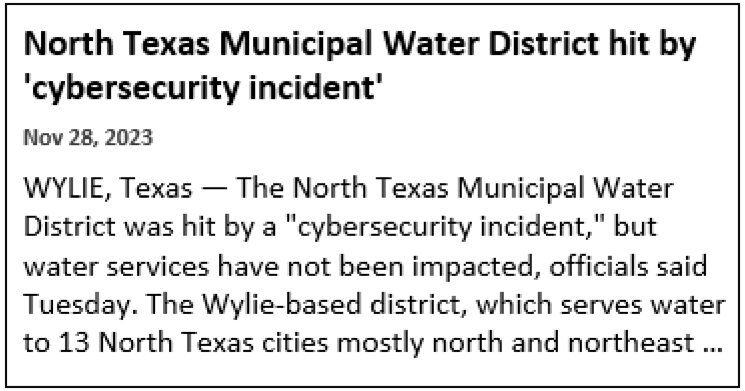
Source FBI IC3 2022 Annual Report

Top 10 Verticals by Intrusion Frequency



Source FBI IC3 2022 Annual Report

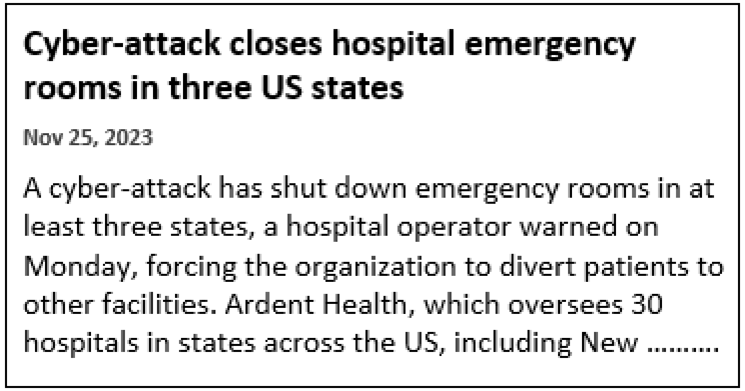
Recent Cyber Attacks in Texas



North Texas Municipal Water District hit by 'cybersecurity incident'

Nov 28, 2023

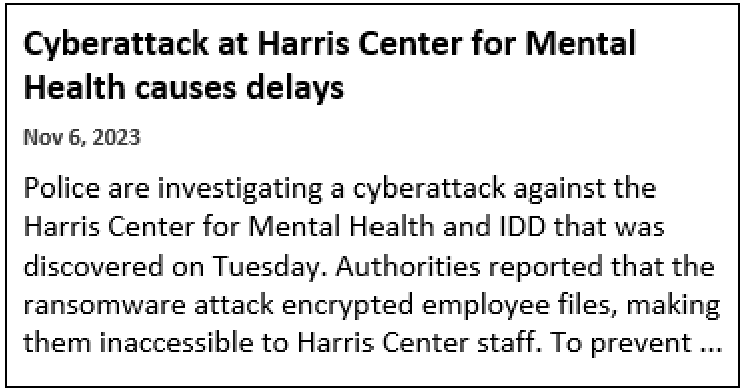
WYLIE, Texas — The North Texas Municipal Water District was hit by a "cybersecurity incident," but water services have not been impacted, officials said Tuesday. The Wylie-based district, which serves water to 13 North Texas cities mostly north and northeast …



Cyber-attack closes hospital emergency rooms in three US states

Nov 25, 2023

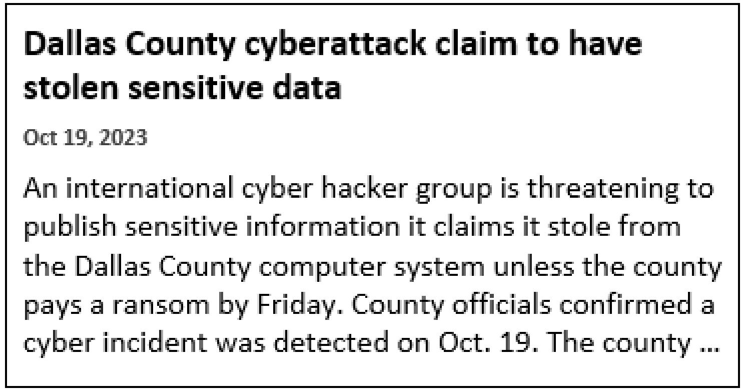
A cyber-attack has shut down emergency rooms in at least three states, a hospital operator warned on Monday, forcing the organization to divert patients to other facilities. Ardent Health, which oversees 30 hospitals in states across the US, including New ……….



Cyberattack at Harris Center for Mental Health causes delays

Nov 6, 2023

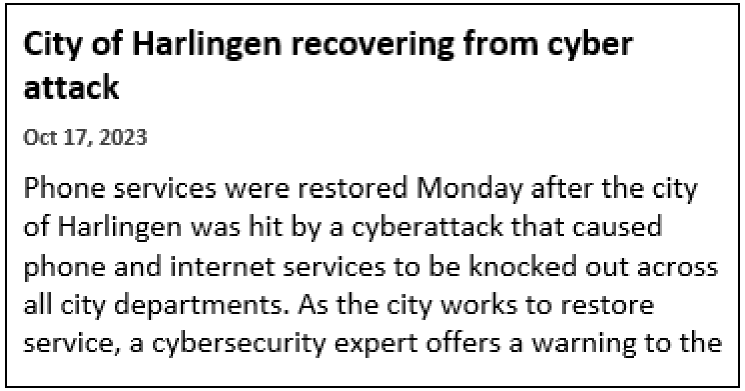
Police are investigating a cyberattack against the Harris Center for Mental Health and IDD that was discovered on Tuesday. Authorities reported that the ransomware attack encrypted employee files, making them inaccessible to Harris Center staff. To prevent …



Dallas County cyberattack claim to have stolen sensitive data

Oct 19, 2023

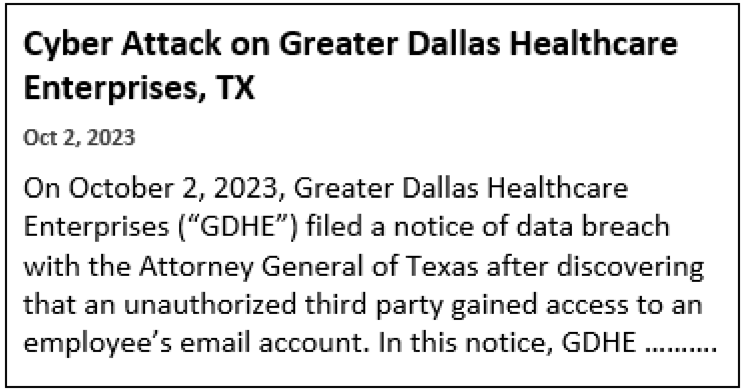
An international cyber hacker group is threatening to publish sensitive information it claims it stole from the Dallas County computer system unless the county pays a ransom by Friday. County officials confirmed a cyber incident was detected on Oct. 19. The county …



City of Harlingen recovering from cyber attack

Oct 17, 2023

Phone services were restored Monday after the city of Harlingen was hit by a cyberattack that caused phone and internet services to be knocked out across all city departments. As the city works to restore service, a cybersecurity expert offers a warning to the



Cyber Attack on Greater Dallas Healthcare Enterprises, TX

Oct 2, 2023

On October 2, 2023, Greater Dallas Healthcare Enterprises ("GDHE") filed a notice of data breach with the Attorney General of Texas after discovering that an unauthorized third party gained access to an employee's email account. In this notice, GDHE ……….

Source FBI IC3 2022 Annual Report

CISA CYBERSECURITY RESOURCES

CISA’s No-Cost Cyber Resources

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

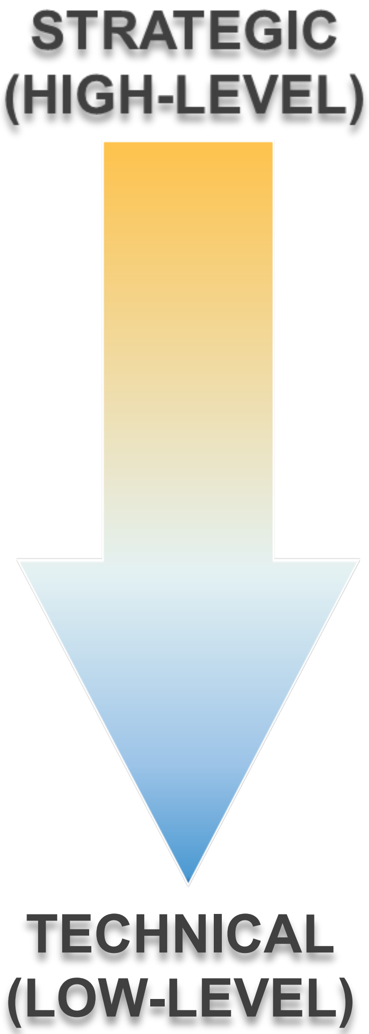
- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)

- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service

- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise (CTTX)

- **Technical Assessments***
  - Remote Penetration Test (RPT)
  - Risk and Vulnerability Assessment (RVA)
  - Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).



STRATEGIC (HIGH-LEVEL)

TECHNICAL (LOW-LEVEL)

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA’s No-Cost Cybersecurity Resources

CISA’s Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

STRATEGIC
(HIGH-LEVEL)

- **Cybersecurity Assessments**
  - ➢ Baseline Assessments
    - ➢ Ransomware Readiness Assessment (RRA)
    - ➢ Cybersecurity Performance Goals (CPG)
  - ➢ Intermediate Assessments
    - ➢ Cyber Infrastructure Survey (CIS)
    - ➢ Cyber Resilience Essentials (CRE)
  - ➢ Advanced Assessments
    - ➢ External Dependencies Management (EDM)
    - ➢ Incident Management Review (IMR)
    - ➢ Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - ➢ External Vulnerability Scanning Service
  - ➢ Web Application Scanning Service

Request CISA’s cybersecurity assessments to **identify your “current state” of cyber** and acquire guidance on how to improve.

Contact your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to schedule these.

TECHNICAL
(LOW-LEVEL)

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

STRATEGIC (HIGH-LEVEL)

- **Cybersecurity Assessments**
  - Baseline Assessments
    - Ransomware Readiness Assessment (RRA)
    - Cybersecurity Performance Goals (CPG)
  - Intermediate Assessments
    - Cyber Infrastructure Survey (CIS)
    - Cyber Resilience Essentials (CRE)
  - Advanced Assessments
    - External Dependencies Management (EDM)
    - Incident Management Review (IMR)
    - Cyber Resilience Review (CRR)
- **Cyber Hygiene Services**
  - External Vulnerability Scanning Service
  - Web Application Scanning Service

Request CISA's external vulnerability scanning service to continuously **identify and address vulnerabilities on internet-facing assets**!

Contact your CISA Cybersecurity State Coordinator or Cybersecurity Advisor (CSA) to get signed up!

TECHNICAL (LOW-LEVEL)

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA's No-Cost Cybersecurity Resources

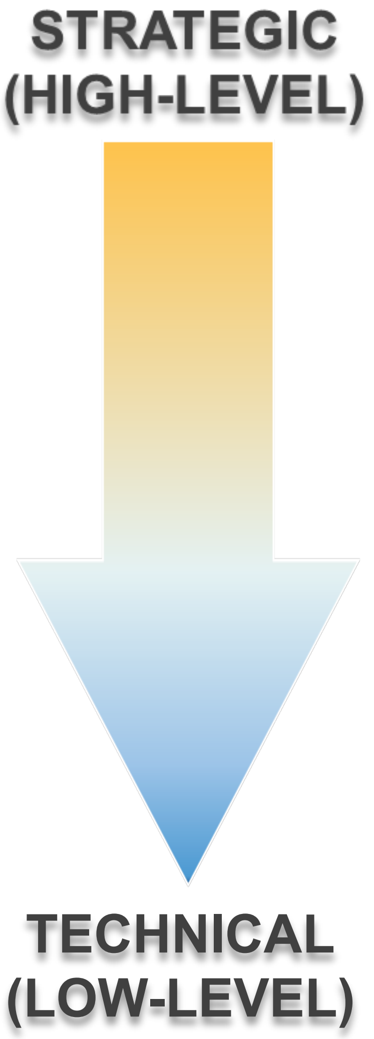
CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

Build new or mature existing cyber capabilities with our workshops.

Exercise your incident response, business continuity, and disaster recovery plans with our Cyber Tabletop Exercise.

Contact your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to schedule these.

- **Workshops & Exercises**
  - Asset Management Workshop (AMW)
  - Cyber Resilience Workshop (CRW)
  - Incident Management Workshop (IMW)
  - Vulnerability Management Workshop (VMW)
  - Digital Forensics Workshop I (DFW I)
  - Digital Forensics Workshop II (DFW II)
  - Cyber Tabletop Exercise

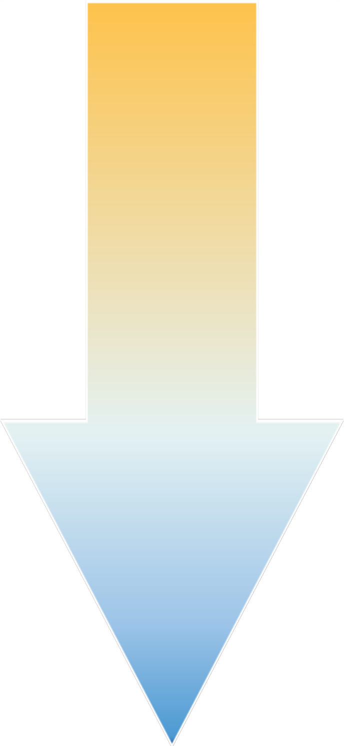


Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

CISA's No-Cost Cybersecurity Resources

CISA's Cybersecurity State Coordinators & Cybersecurity Advisors (CSAs)

STRATEGIC (HIGH-LEVEL)



TECHNICAL (LOW-LEVEL)

- Cybersecurity Assessments
  - ➢ Baseline Assessments
    - ➢ Ransomware Readiness Assessment (RRA)
    - ➢ Cybersecurity Performance Goals (CPG)
  - ➢ Intermediate Assessments
    - ➢ Cyber Infrastructure Survey (CIS)

- Workshops & Exercises
  - ➢ Asset Management Workshop (AMW)
  - ➢ Cyber Resilience Workshop (CRW)
  - ➢ Incident Management Workshop (IMW)
  - ➢ Vulnerability Management Workshop (VMW)
  - ➢ Digital Forensics Workshop I (DFW I)
  - ➢ Digital Forensics Workshop II (DFW II)

Work with your CISA Cybersecurity State Coordinator (CSC) or Cybersecurity Advisor (CSA) to assess eligibility for our technical assessments, including the RPT, RVA, VADR, and more.

- **Technical Assessments***
  - ➢ Remote Penetration Test (RPT)
  - ➢ Risk and Vulnerability Assessment (RVA)
  - ➢ Validated Architecture Design Review (VADR)

***Note:** Eligibility for technical assessments is contingent upon assessment of the stakeholder's capabilities by their Cybersecurity Advisor (CSA).

Cybersecurity State Coordinator (TX): ernesto.ballesteros@cisa.dhs.gov

Next Steps

Forming a Partnership with CISA on Cybersecurity Matters

Next Steps: CISA Cyber Partnership

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

Next Steps:

1. Contact your CISA Regional Office (CISARegion6@cisa.dhs.gov);
2. Request to schedule initial Cyber Protective Visit (CPV) from your Cybersecurity Advisor (CSA) or Cybersecurity State Coordinator (CSC); and
3. Meet with your CSA/CSC and discuss how they can provide these assessments, workshops, exercises, and technical services for your organization.

Email: todd.vasilou@cisa.dhs.gov

CISA Regions: https://www.cisa.gov/cisa-regions

CISA Regions 6: CISARegion6@cisa.dhs.gov

CISA REGION 6

Todd Vasilou
Cybersecurity Advisor
Cybersecurity and Infrastructure Security Agency
EMAIL: todd.vasilou@cisa.dhs.gov
CELL: (210) 422-0128

CISA Region 6
CISARegion6@cisa.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)
(855) 292-3937; CyWatch@fbi.gov