RANSOMWARE 101 AND CISA'S PRE-RANSOMWARE NOTIFICATION INITIATIVE (PRNI)

Rob Main, CGCIO
Cybersecurity State Coordinator (NC)
US Department of Homeland Security
Cybersecurity and Infrastructure Security Agency – Region IV

TLP:GREEN

INTRODUCTION

Rob Main

- 34+ years of experience in Information Technology and Cybersecurity
- Certified Government Chief Information Officer – UNC-CH
- Masters of Business Administration – ECU
- Bachelor of Computer Science Degree – Troy University
- 25-Year military veteran (USAF and NC Air National Guard)

CYBERSECURITY &
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

TLP: GREEN

Divisions of CISA

CYBERSECURITY DIVISION

INTEGRATED OPERATIONS DIVISION

INFRASTRUCTURE SECURITY DIVISION

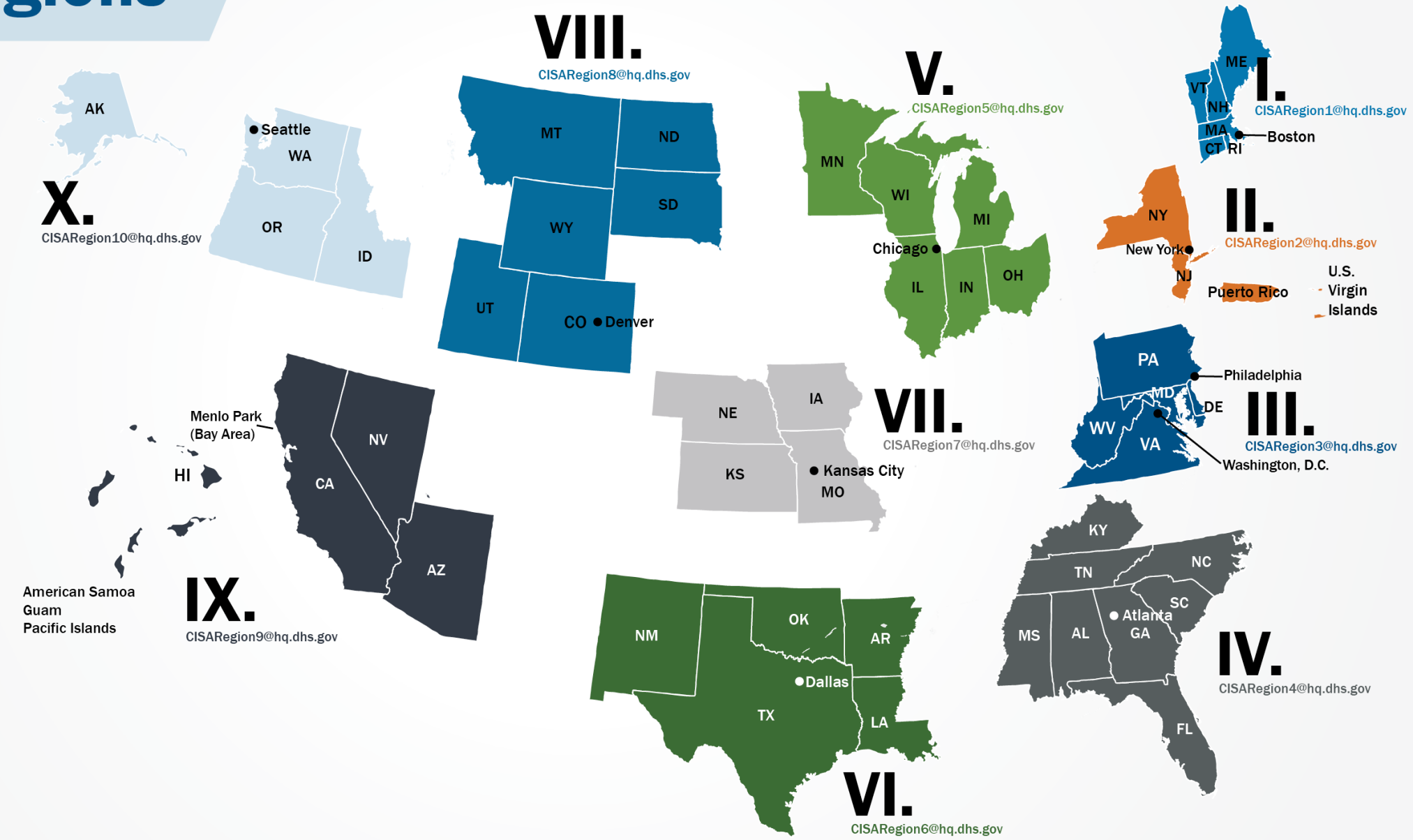
NATIONAL RISK MANAGEMENT CENTER

EMERGENCY COMMUNICATIONS DIVISION

STAKEHOLDER ENGAGEMENT DIVISION

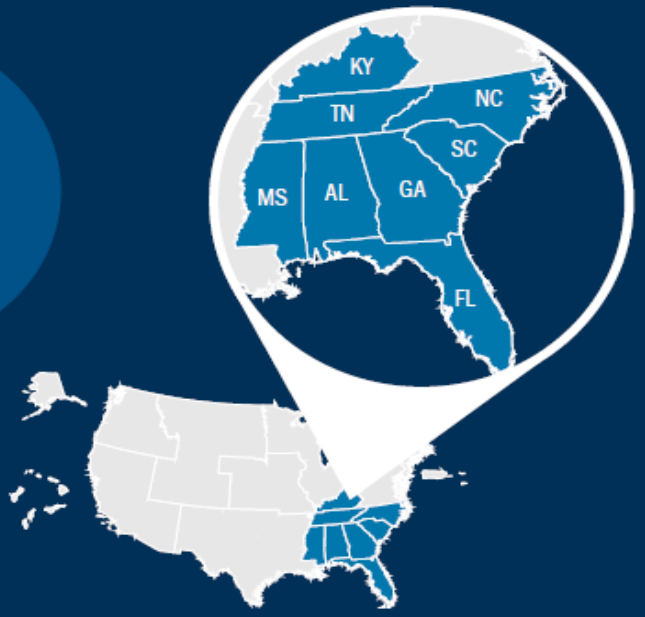
TLP:GREEN

CISA Regions



- I — Boston, MA
- II — New York, NY
- III — Philadelphia, PA
- IV — Atlanta, GA
- V — Chicago, IL
- VI — Irving, TX
- VII — Kansas City, MO
- VIII — Lakewood, CO
- IX — Oakland, CA
- X — Seattle, WA
- CS — Pensacola, FL

CISA
CYBER+INFRASTRUCTURE



CYBERSECURITY + INFRASTRUCTURE SECURITY AGENCY

REGION IV

REGION IV AT-A-GLANCE

REGIONAL OFFICE:
ATLANTA, GEORGIA

LOCATION:
8 STATES
6 TRIBAL NATIONS

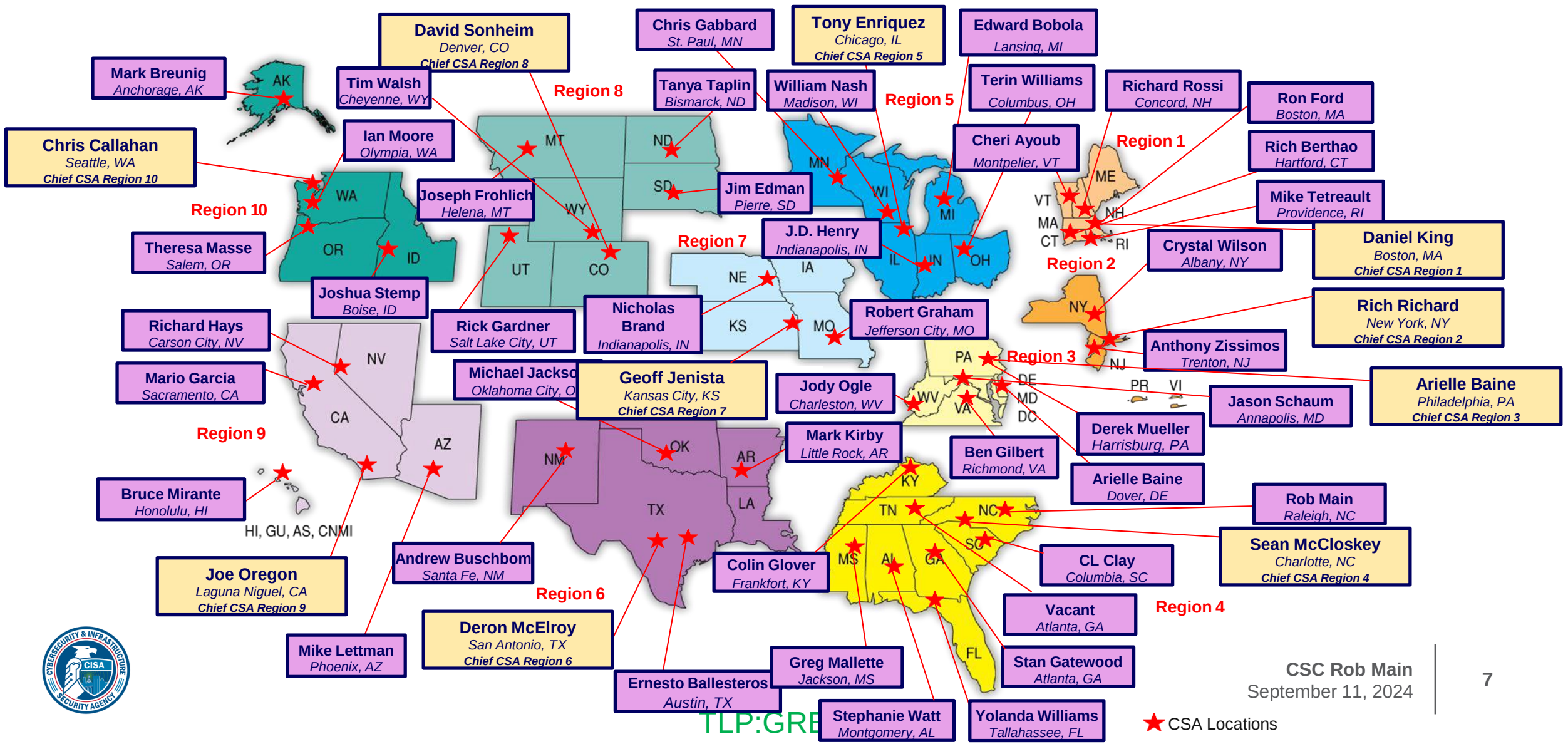
SIZE:
394,420 SQUARE MILES

ESTIMATED POPULATION:
65.733 MILLION

KEY FACTS:

- Contains 17 nuclear power facilities (with applications for nine new sites pending). These facilities supply 29 percent of the nation's electrical power output
- Harbors six nationally critical ports
- Home to 7 of the country's fastest growing cities: Orlando, FL; Nashville, TN; Cape Coral, FL; West Palm Beach, FL; North Port, FL; Lakeland, FL; and Raleigh, NC (2018 data).

Cybersecurity Chiefs and Coordinators



Today's Risk Landscape

America remains at risk from a variety of threats:

INSIDER THREAT

ACTS OF TERRORISM

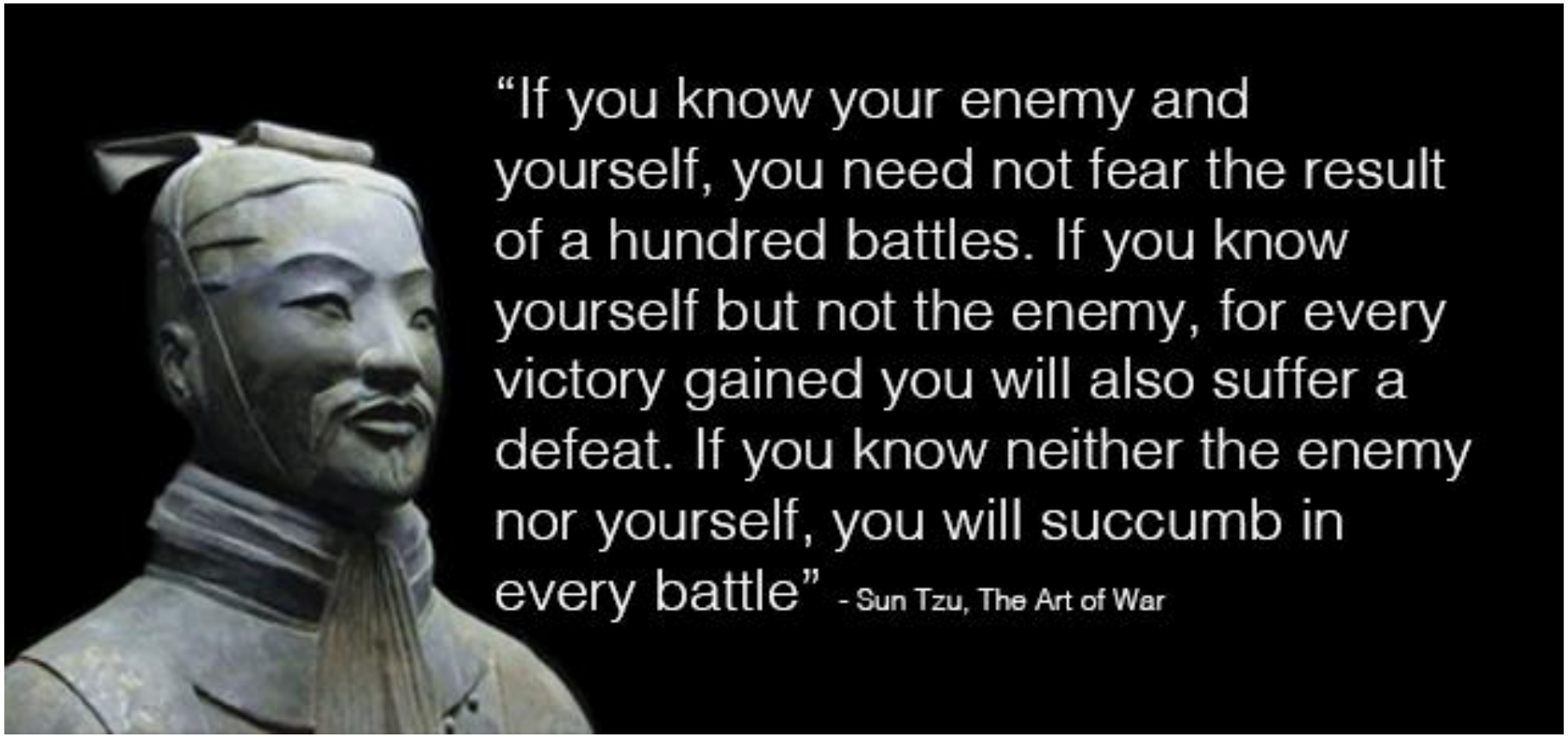
CYBER ATTACKS

EXTREME WEATHER

PANDEMICS

ACCIDENTS OR TECHNICAL FAILURES

Know Thy Enemy



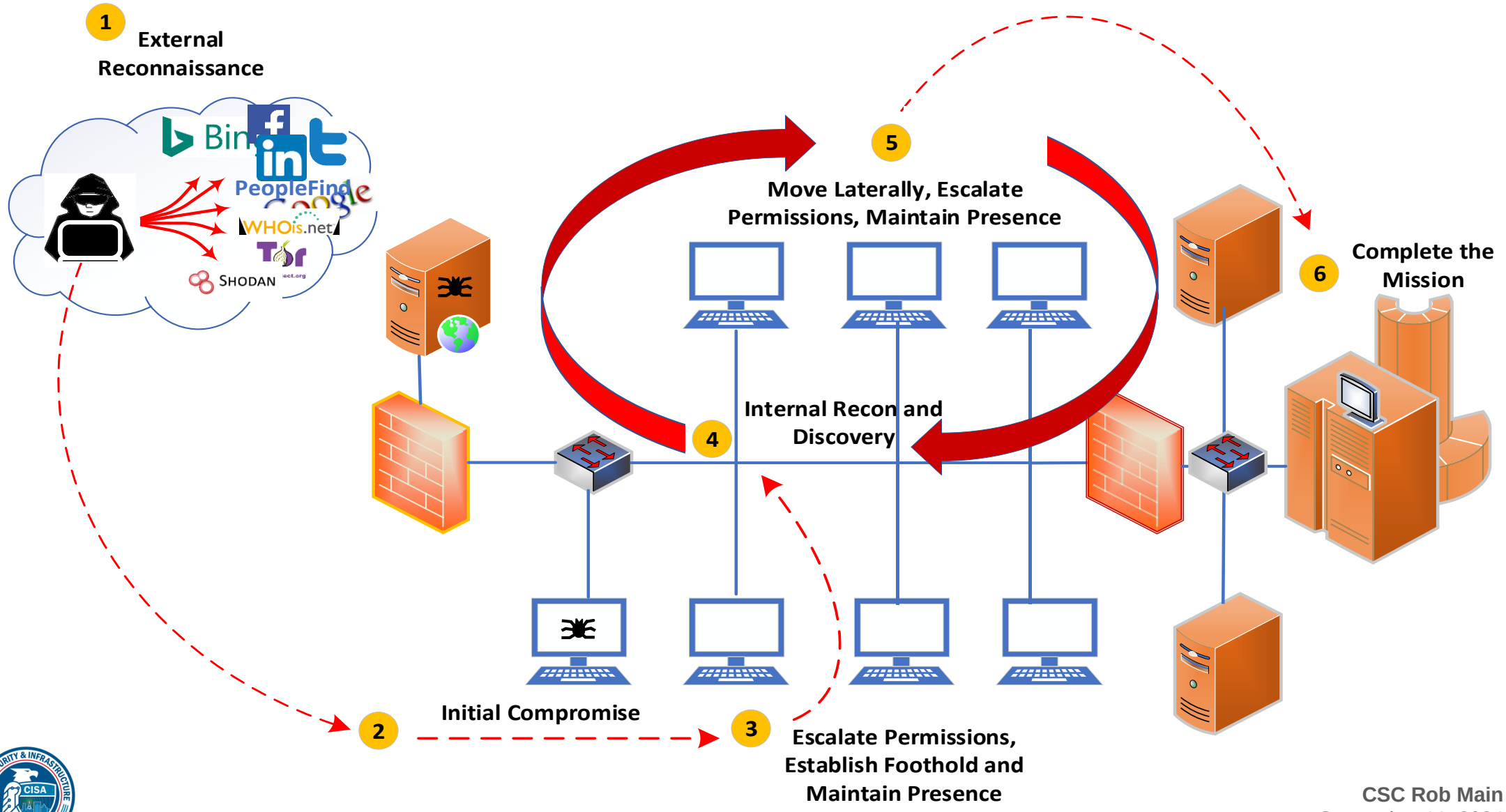
TLP:GREEN

Cyber Threat Actors

Who They Are and How They Achieve Their Objective

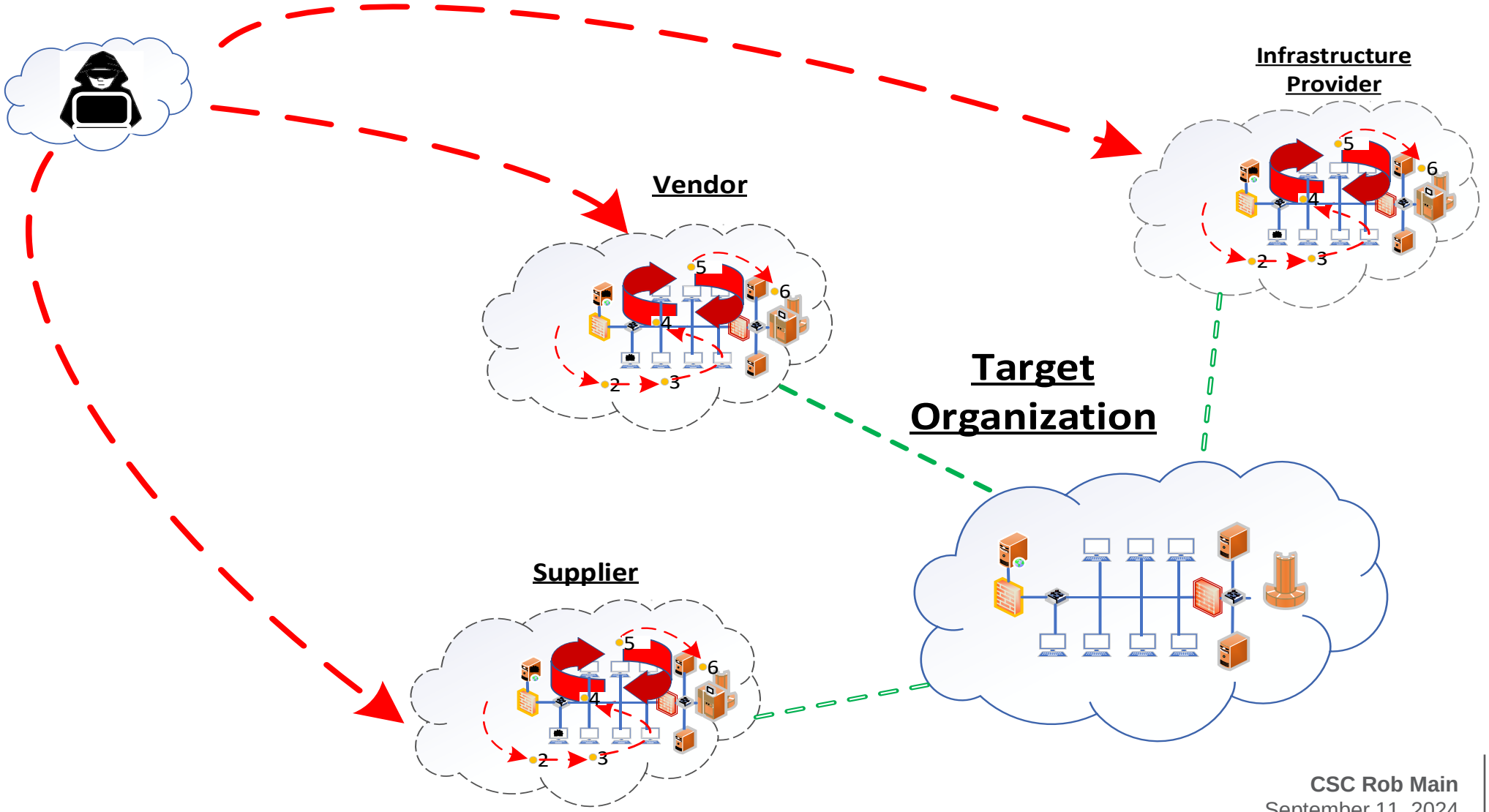
- Malicious groups or individuals who aim to exploit weaknesses in an information system, or to exploit its operators to gain unauthorized access to or otherwise affect victims' data, devices, systems, and networks.
- They pursue their objectives by exploiting technical vulnerabilities, using social engineering, and by creating, disseminating, or amplifying false or misleading content online to influence individuals' behavior and beliefs.

Mechanics of a Cyber Attack - 1



TLP:GREEN

Mechanics of a Cyber Attack - 2



TLP:GREEN

Beyond the Headlines: What is Ransomware?

Ransomware 101

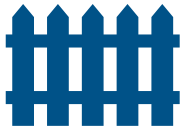
Ransomware is a form of malware designed to encrypt files on a device, rendering any files and the systems that rely on them unusable.

Malicious actors then demand ransom in exchange for decryption.

How to Prepare for, Mitigate Against

Preparation phase: How are staff trained and prepared? What tools and resources are they armed with to respond to ransomware incidents? Consider awareness and education for users here.

Identification phase: How do you recognize and detect a ransomware incident? How do you go about understanding the strain of ransomware, attack vector, and attack group through gathering data and performing initial analysis?



Containment phase: For ransomware incidents, it is imperative that infected systems are quickly contained to limit the damage. How will you contain the incident from spreading to network shares and other connected devices?

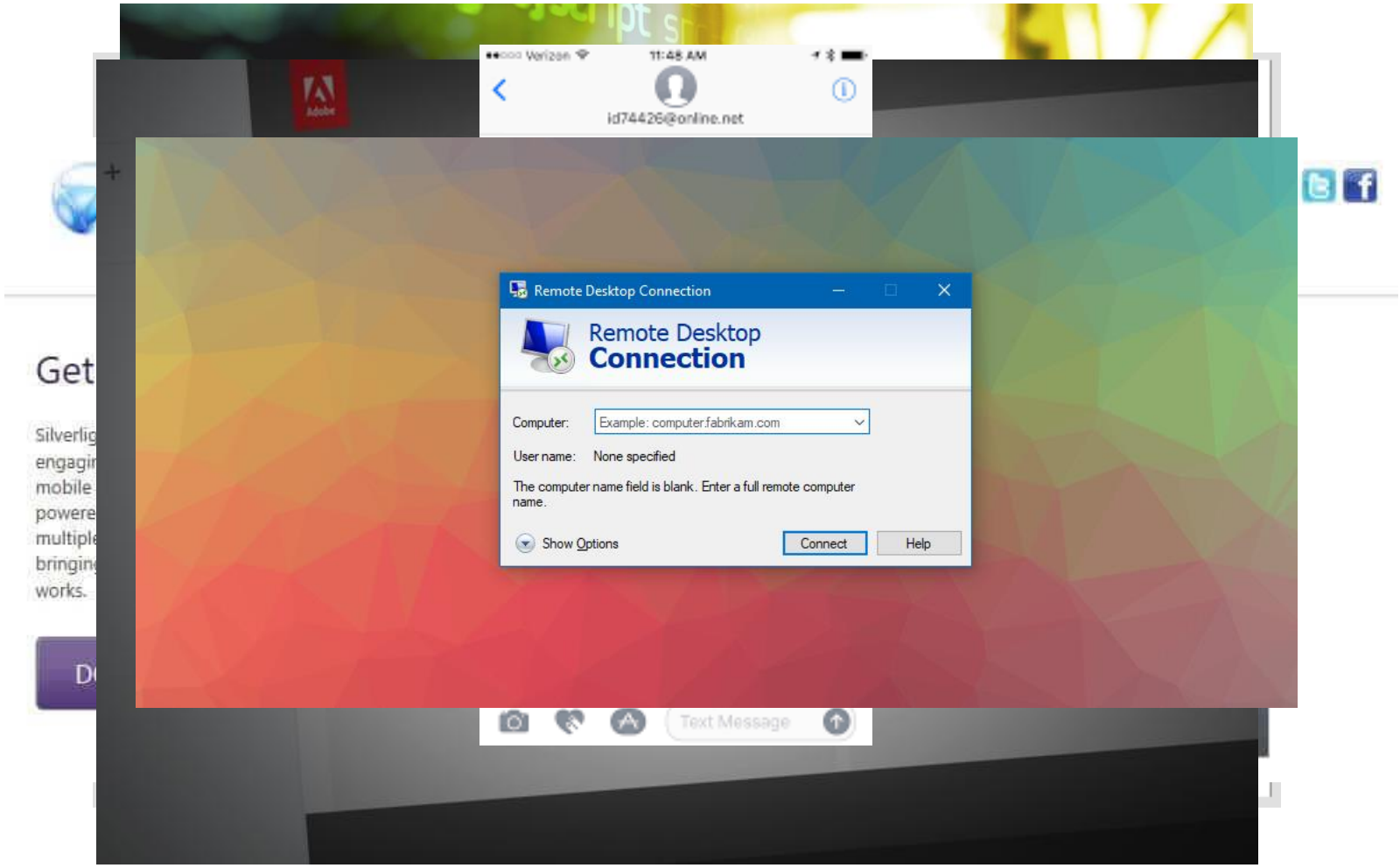
Infects…Encrypts…Extorts

- Ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver mission-critical services.
- Malicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.
- The monetary value of ransom demands has also increased, with demands for millions of dollars becoming commonplace.
- Ransomware incidents have become more destructive and impactful in nature and scope.

Methods of Infection

The following can all be vectors of infection for ransomware attacks:

- Phishing
- Compromised Websites
- Malvertising
- Exploit Kits
- Downloads
- Messaging Applications
- Brute Force via RDP



Trend: Ransomware-as-a-Service (RaaS) Model

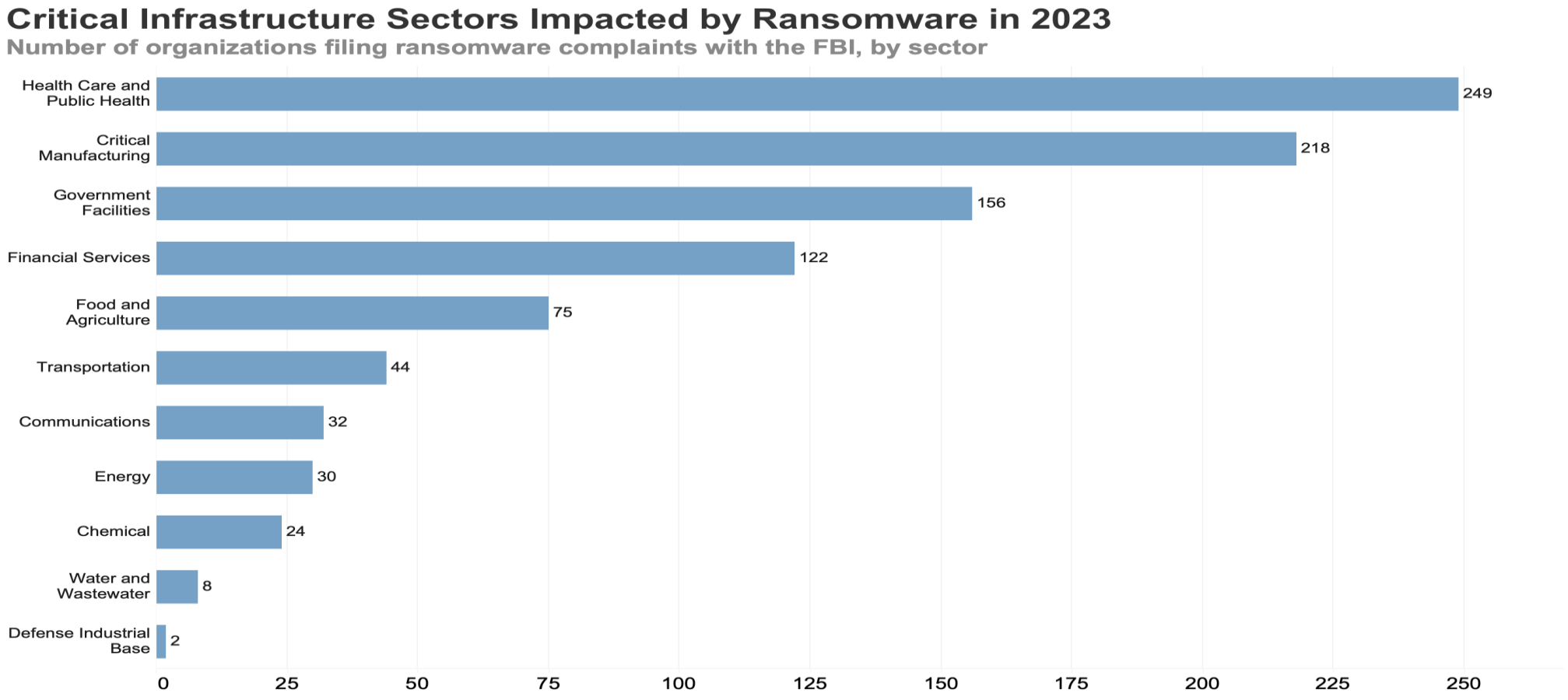
- Ransomware families selling RaaS to other cybercriminals
- Popularity increases → Barriers to entry drop, becomes scalable, more efficient.
- Enables relatively unskilled bad actors to access complex tools and the environment from which to run their campaigns.

- The "commoditization" of the ransomware threat: Entrepreneurial Operators, including NetWalker, Nefilim, and Sodinokibi/REvil all provide access to partners in pre-agreed profit-sharing arrangements.
- Increased investment in many of the platforms themselves, upgrading their core ransomware systems to stay ahead of the good guys and evade detection.

Trend: Double Extortion

- **Weaponized**: One part Ransomware, One Part Data Breach
- **Old Paradigm**: Victim's data encrypted, actor locks victim out of their own files. If victim refuses to pay the ransom, the actor destroys their files.
- **New Paradigm**:
  - Attacker exfiltrates data (e.g., large quantities of sensitive proprietary or sensitive information,) before encryption.
  - Attacker threatens to publish unless ransom paid, often will release small portions of data online.
  - If negotiation goes badly, attacker publishes all data and/or sells to a third party – putting added pressure on enterprises to meet the hackers' demands.

Critical Infrastructure Impact

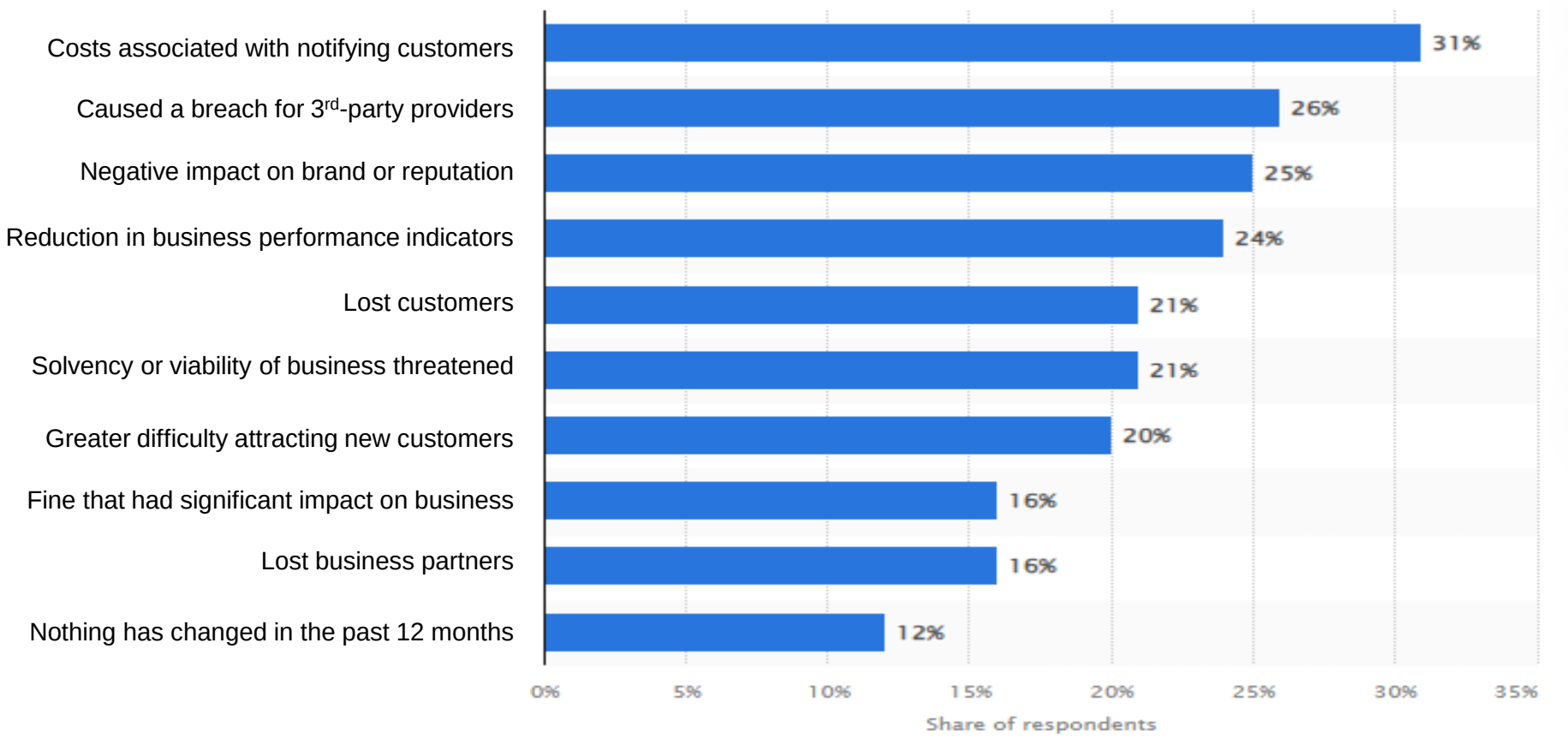


Note: Data from FBI Internet Crime Report 2023. The number of complaints is likely an underestimate of the true number of ransomware victims as many infections go unreported to law enforcement.

EconoFact: econofact.org

TLP:GREEN

Consequences of Cyber Attacks



Source: Statista 2024

TLP:GREEN

Change Healthcare Breach – 21-Feb-2024

- **What We Know:**
  - BlackCat/ALPHV attackers loitered on Change Healthcare systems for **nine days** before deploying ransomware
  - Initial access gained through Change Healthcare Citrix portal by leveraging compromised credentials (**MFA not enabled**)
  - **Lack of/poor segmentation** allowed attackers the freedom of movement for additional internal discovery
  - UHG (acquired Change in Oct '22) was **self-insured** and incurred **$872M in IR&R costs**
  - **Double extortion** involving the **ransom payment of $22M** for decryption and **additional payment to prevent the release of exfiltrated data**
  - **Delay in claims processing* costs exceeded $6B** for approximately 900,000 physicians, 33,000 pharmacies, 5,500 hospitals, and 600 laboratories (* half of all US claims)

TLP:GREEN

CISA's Pre-Ransomware Notification Initiative (PRNI)

- **CISA collaborates with the cybersecurity research community, infrastructure providers, and cyber threat intelligence companies to receive tips on potential early-stage ransomware activity**
- Ransomware actors often take some time after gaining initial access to a target before encrypting or stealing information, a window of time that often lasts from hours to weeks. This window gives CISA time to warn organizations that ransomware actors have gained initial access to their networks.
- These early warnings can enable affected organizations to safely evict the ransomware actors from their networks before the actors have a chance to encrypt and hold critical data and systems at ransom
- These notifications can also significantly reduce potential loss of data, impact on operations, financial ramifications, and other detrimental consequences of ransomware deployment

Impact of the PRNI Program

- Prevent ransomware incidents
- Prevent ransomware actors from making business models sustainable
- Limit the social harm that results from successful encryption
  - citizens, customers, and cybersecurity teams
- Drive public-private collaboration for scalable disruption of ransomware groups
- **BUILD TRUST**

✓ **1,213** Pre-Ransomware Notifications in 2023

✓ **1,600+ so far in 2024**

✓ **40** International Governments Notified

CISA Notification Process

1
- Build Partnerships with researchers and CTI teams who provide regular, high-confidence tipping of pre-encryption ransomware gang or initial access broker intrusions

2
- CISA conducts basic vetting of tip, and sends a notification with tailored hunt guidance via regional cyber personnel **or** international CERT partner to affected organization

3
- Regional cyber personnel or National CERT conducts out-of-band notification. CISA HQ supports follow up questions and specialized assistance.

??
- Stop ransomware and share feedback from affected entity.
  - Share tactics, techniques and procedures to broaden understanding of the threat actors and disrupt ransomware:
    - CISA Advisories
    - Known Exploited Vulnerability (KEV) Catalog Updates
    - Ransomware Vulnerability Warning Pilot (RVWP)

Intrusion Vectors/Initial Access

Theft of Legitimate Credentials:

- Phishing, including Phishing as a Service kits that also steal session cookies
- Stealer logs harvested for credentials

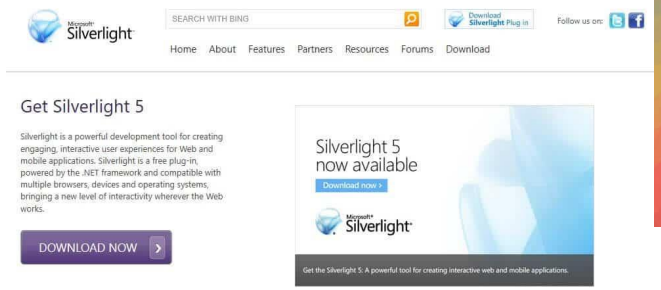
Exploitation of Internet-facing Vulnerabilities:

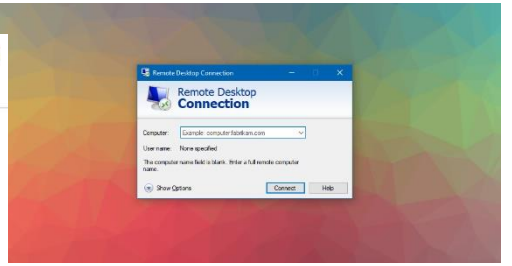
- Threat actors usually use a public proof of concept
- Commonly VPNs and other edge devices

Pre-existing Malware Infections:

- Malvertising and imposter installers or app downloads
- Exploitation of web vulnerabilities to facilitate search engine optimization (SEO) poisoning that enables threat actors to obtain malware infections

Remote Desktop Protocol (RDP) Brute Forcing





TLP:GREEN

How to Respond to, and Recover From

Eradication phase: How will you perform a forensic analysis of data to determine the cause of the incident, remove the ransomware from infected devices, patch vulnerabilities and update protection?

Recovery phase: How will you return to normal operation? Re-imaging or restoring from backup may not work if the ransomware lay dormant during the last image or backup cycle, or if part of the ransomware attack was to seek and destroy back-ups.

Post-Incident phase: After the incident is resolved, what can you learn to prevent it from happening again in the future? How will you document the incident? Detail improvements to IR plans, additional security controls, preventative measures or new security initiatives?

Executive Decision-Making Considerations

CISA encourages organizations to develop a Ransomware Playbook that provides the practices for response as well as illustrates critical points for executive leadership involvement, including how to respond. Executives will have many considerations, including:

- Recommendations from in-house Legal Counsel, Board, etc.
- The impact of maintaining manual operations without interrupting business services.
- The impact to partner systems and operations.
- Do we have Cyber Insurance coverage?
- Reputational/Brand risk exposure.
- Financial risk and legal cost/benefit analysis

USG strongly recommend against paying ransom

Call to Action

- Review the CISA Stop Ransomware Guide
- Adopt the Cybersecurity Performance Goals (CPG), such as:
  - Mitigate Known Vulnerabilities (apply system patches) (1.E)
  - Network segmentation (2.F)
  - Use Phishing-Resistant Multifactor Authentication (MFA) (2.H)
  - Deploy security.txt files (4.C)
- Enroll in CISA's no-cost Cybersecurity Services
  - Cyber Hygiene (CyHy) Vulnerability Scanning
- Remain aware of the latest alerts and advisories CISA provides in response to emerging vulnerabilities and threat activity

CISA Resources

- CISA Stop Ransomware
  - CISA Stop Ransomware Guide
  - Report Ransomware
- CISA RVWP
- CISA PRNI
- Joint Ransomware Task Force (JRTF)
- CISA KEV Catalog
  - CISA BOD 22-01 [KEV Catalog] FAQs
  - Additional KEV information
- CISA CPGs
- CISA Alerts & Advisories

TLP:GREEN

Incident Reporting

Why report cyber incidents?

- For situational awareness
- For decision making
- Requesting response assistance

When to report a cyber incident?

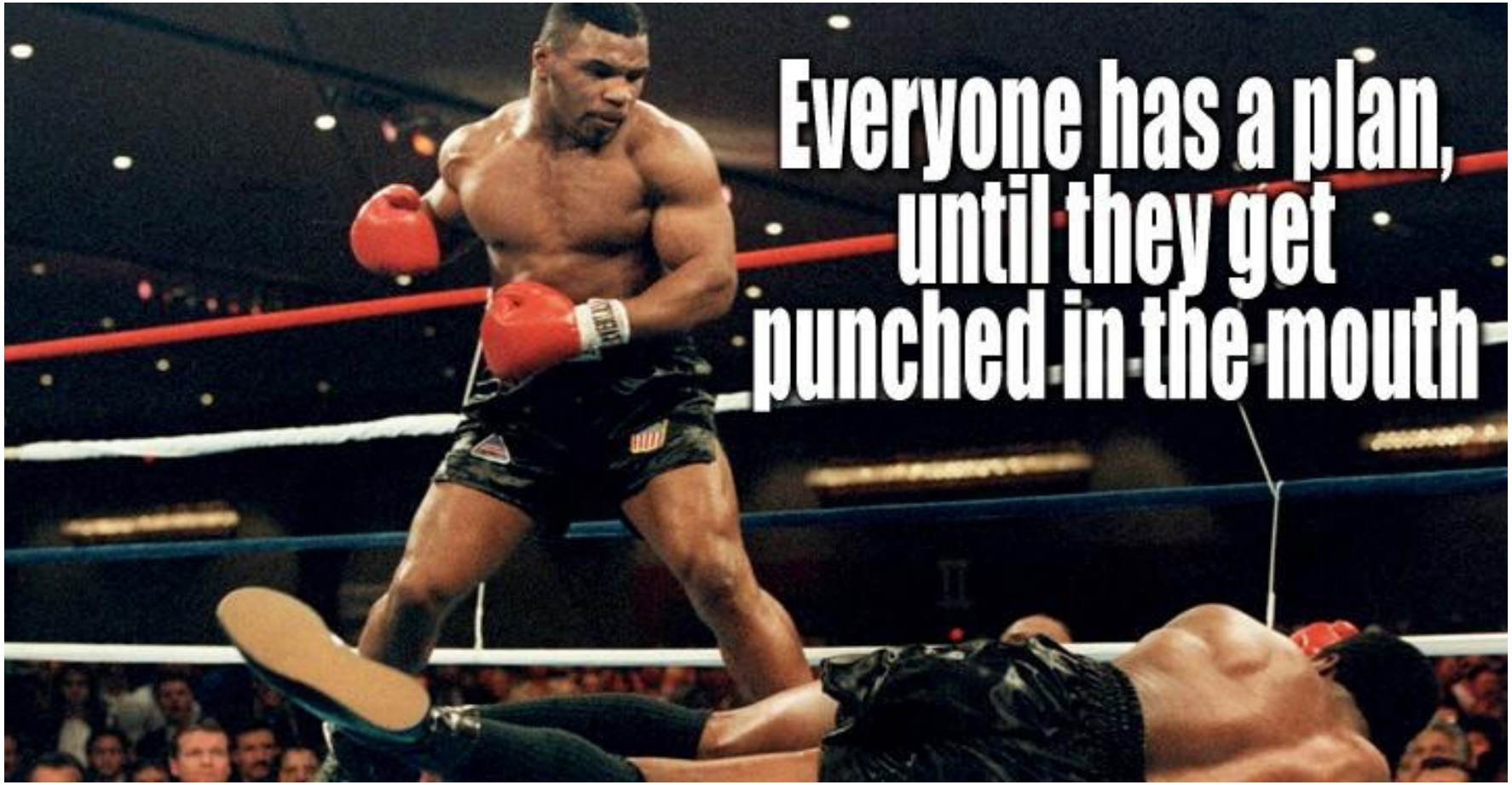
If there is a suspected or confirmed cyber attack or incident that:

- Affects core or critical business functions;
- Results in the loss of data, system confidentiality, integrity, and/ or availability; or control of systems;
- Indicates malicious software is present on critical systems

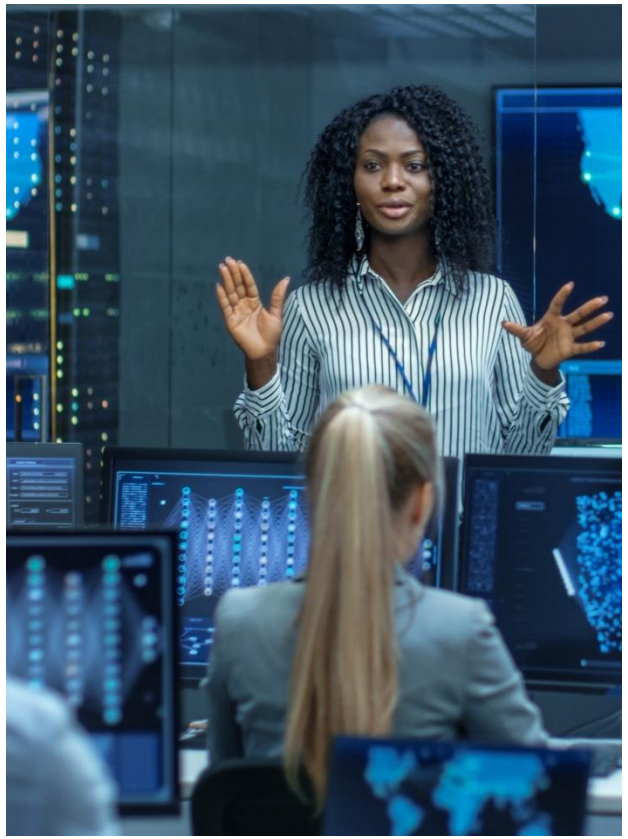
Who to report cyber incidents to?

- Leadership, public affairs, legal and other internal stakeholders
- Relevant vendors
- Law enforcement and other government agencies
- Cyber insurance providers
- Appropriate 3rd party incident response teams

Bottom Line



Contact



General Inquiries

CISARegion4@hq.dhs.gov

CISA Contact Information

Rob Main **CSC - Raleigh NC** **CISA Region 4**	**Rob.Main@cisa.dhs.gov**

CISA Resource Hub

https://www.cisa.gov/cyber-resource-hub


CYBERSECURITY & INFRASTRUCTURE
CISA
SECURITY AGENCY