South Dakota Department of Agriculture & Natural Resources

U.S. Department of Homeland Security

CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Shane Hoenke
Cyber Security Advisor
South Dakota

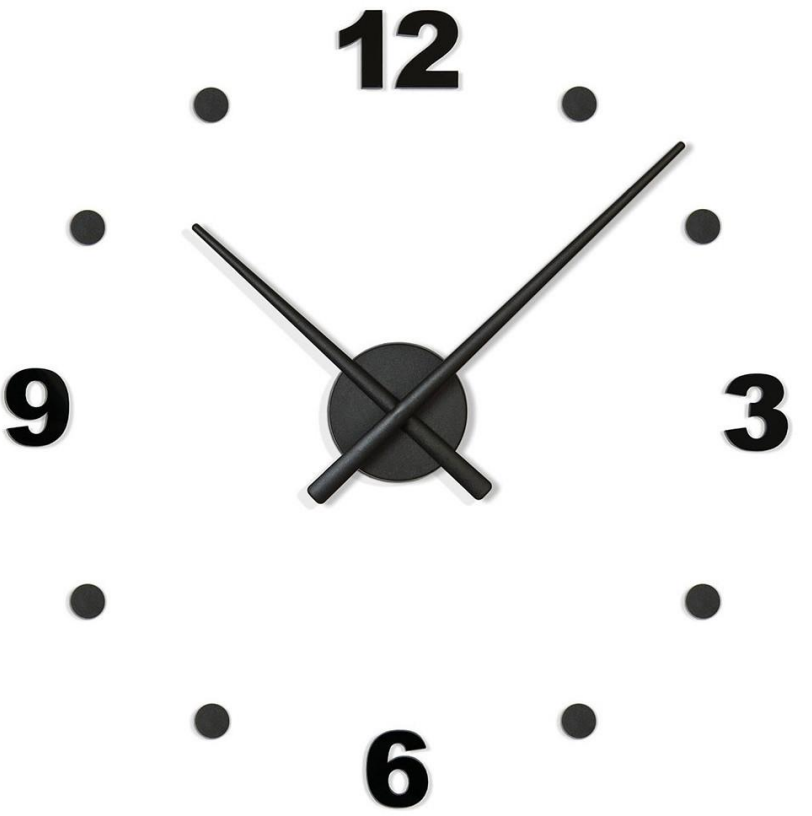
Jim Edman
Cyber Security Coordinator
South Dakota

July 2023

Are you Above or Below the Cybersecurity Poverty Line?

Agenda

- What is CISA?
- The Internet
- Risks, Threats & Consequences
- Ransomware
- Breaches
- Best Practices



Message Takeaways

Prioritize Cybersecurity

Recognize the Risk

Free CISA Resources

Proactive wins over Reactive

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Cybersecurity and Infrastructure Security Agency (CISA)

VISION

A secure and resilient critical infrastructure for the American people.

MISSION

Lead the National effort to understand and manage cyber and physical risk to our critical infrastructure.

CISA is the Nation's lead civilian cybersecurity agency and the national coordinator for critical infrastructure security and resilience efforts.

Who We Are:

Cybersecurity

Infrastructure Security

Emergency Communications

Chemical Security

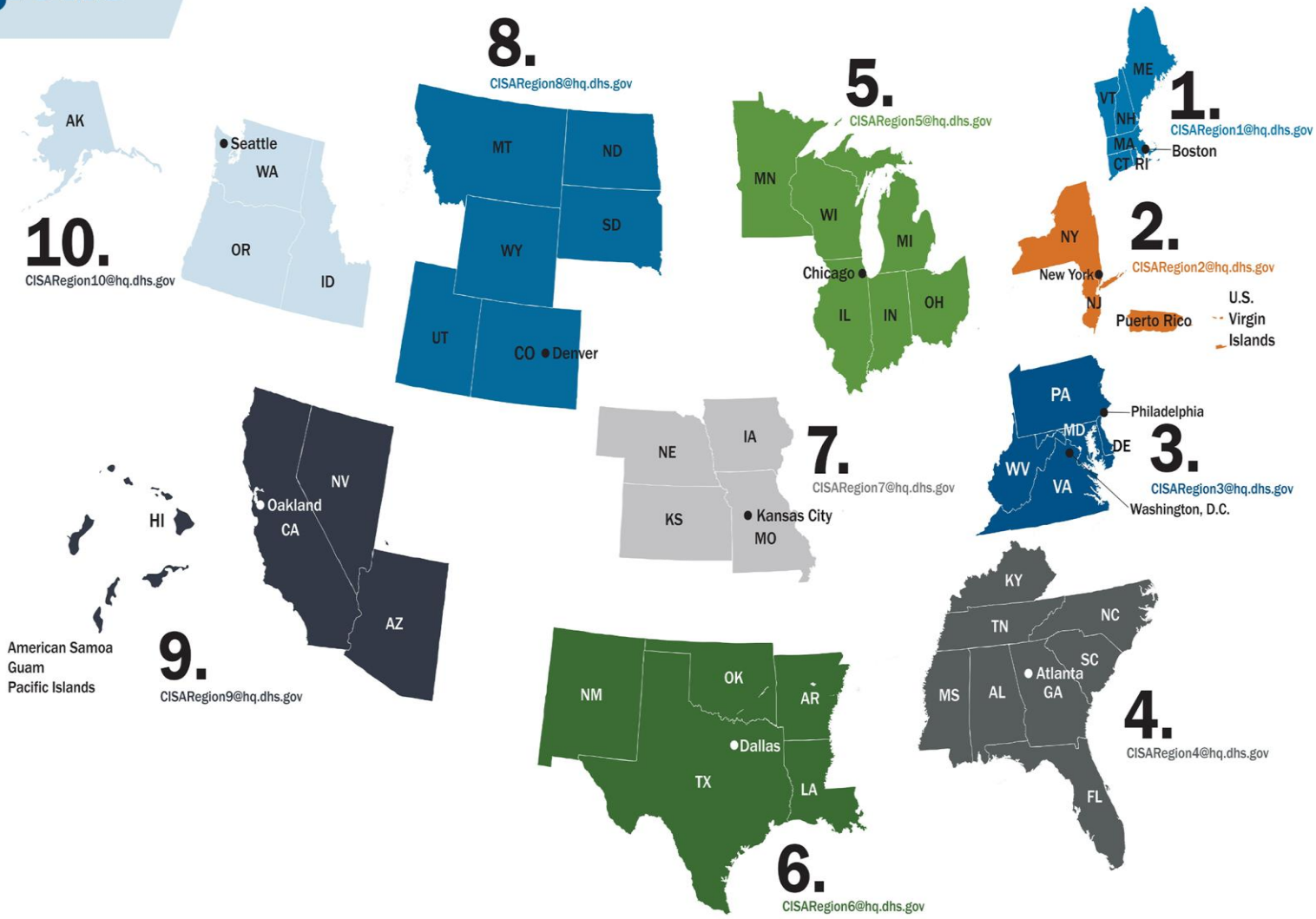
National Risk Management Center

Serving Critical Infrastructure

These 16 sectors underpin the essential services of our Nation's economy, security, and health.
CISA serves as the lead agency for 8 of the sectors.

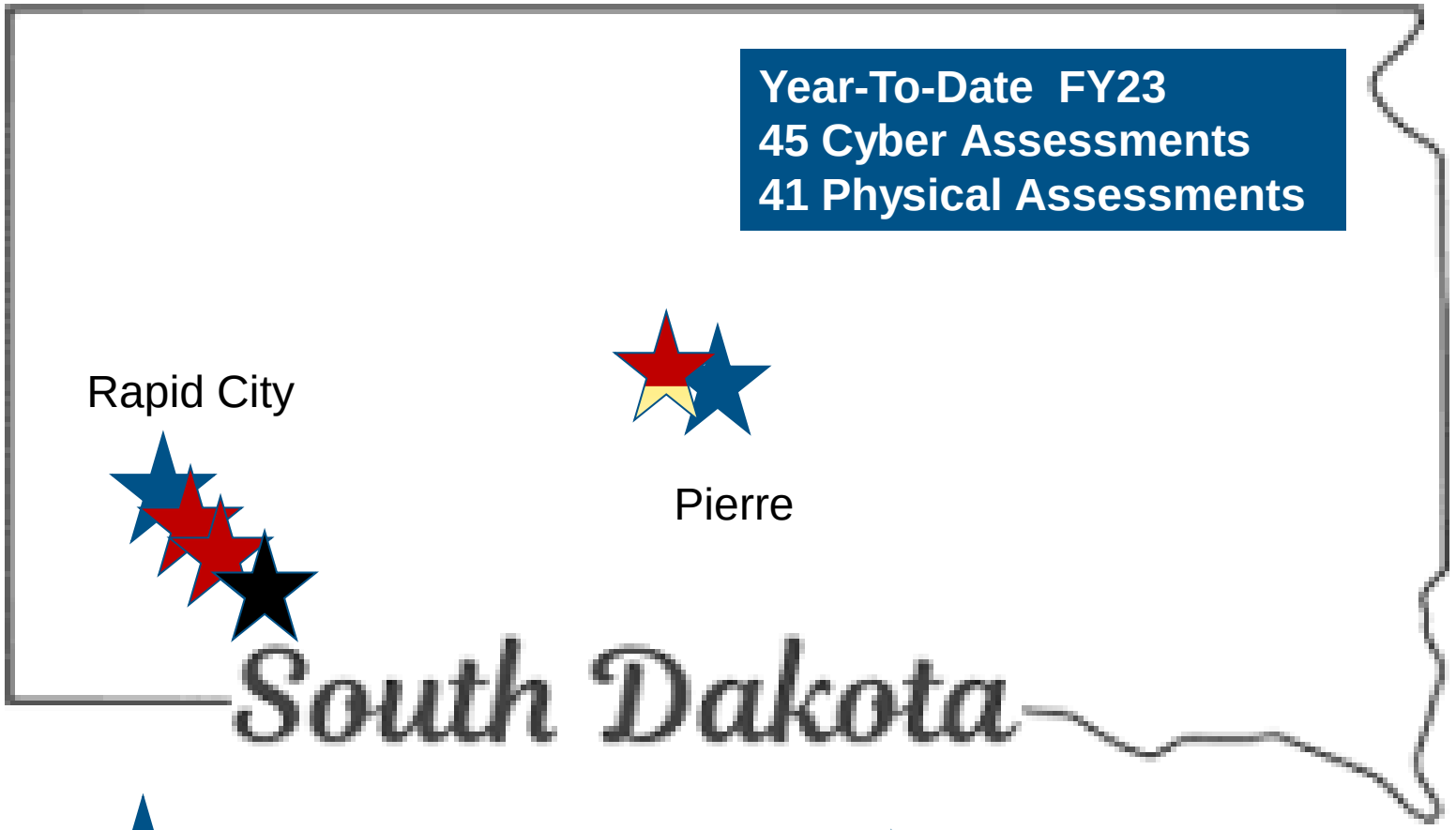
CHEMICAL	CISA
COMMERCIAL FACILITIES	CISA
COMMUNICATIONS	CISA
CRITICAL MANUFACTURING	CISA
DAMS	CISA
DEFENSE INDUSTRIAL BASE	DOD
EMERGENCY SERVICES	CISA
ENERGY	DOE
FINANCIAL	Treasury
FOOD & AGRICULTURE	USDA & HHS
GOVERNMENT FACILITIES	GSA & FPS
HEALTHCARE & PUBLIC HEALTH	HHS
INFORMATION TECHNOLOGY	CISA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

CISA Regions



1	Boston, MA
2	New York, NY
3	Philadelphia, PA
4	Atlanta, GA
5	Chicago, IL
6	Irving, TX
7	Kansas City, MO
8	Lakewood, CO
9	Oakland, CA
10	Seattle, WA
CS	Pensacola, FL

CISA in South Dakota



Cybersecurity Advisor

Protective Security Advisor

Chemical Security Inspector

Cybersecurity Advisor Program

To provide direct coordination, outreach, and regional support and assistance in the protection of cyber components essential to the Nation's Critical Infrastructure.

Protective Security Advisors

Protective Security Advisors (PSA) have five mission areas directly supporting the protection of critical infrastructure:

- Plan, coordinate, and conduct security surveys and assessments
- Plan and conduct outreach activities – public & private sector
- Support National Special Security Events (NSSEs) & Special Event Activity Rating (SEAR) events
- Support state and federal partners with critical infrastructure recovery post-incident
- Coordinate and support improvised explosive device awareness and risk mitigation training & assessments

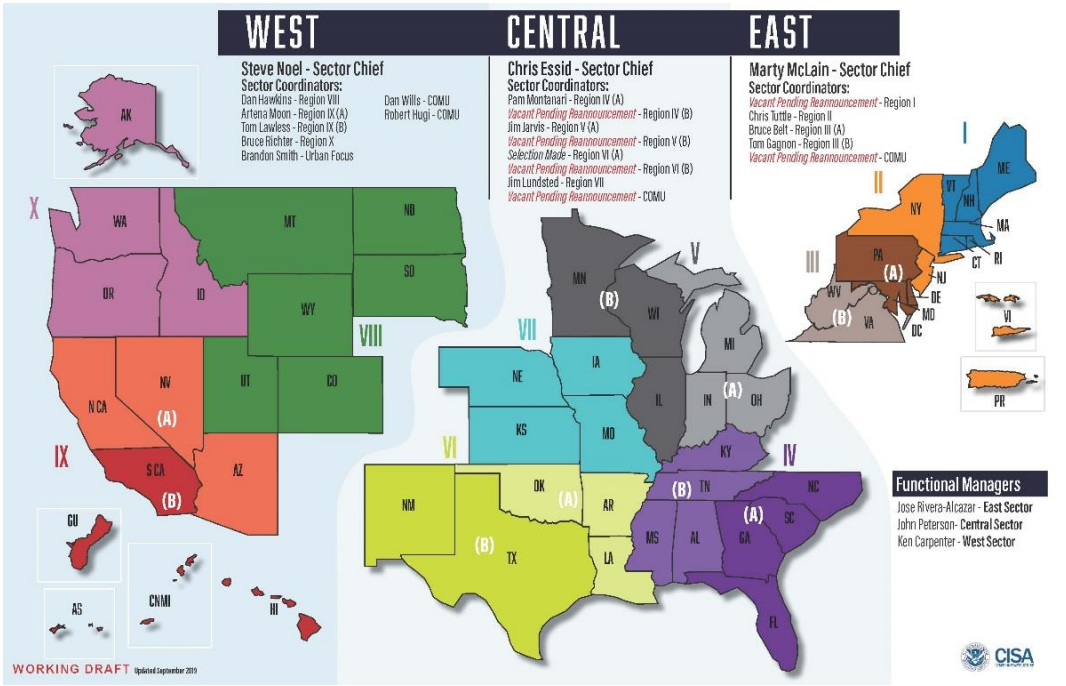
Chemical Security Inspectors

Chemical Security Inspectors visit chemical facilities to ensure that they meet the security requirements set forth by the Chemical Facility Anti-Terrorism Standards (CFATS) Regulatory Security Program. The CFATS program identifies and regulates high-risk Chemical facilities to ensure they have security measures in place to reduce the risk that certain hazardous chemicals are not weaponized by terrorists.

- **Plan, coordinate, and conduct regulatory Inspections and Compliance Assistance Visits**
- **Plan & Conduct Outreach engagement activities**
- **Support Enforcement Operations**
- **Support Chemical sector security events**

Emergency Communications Coordinators

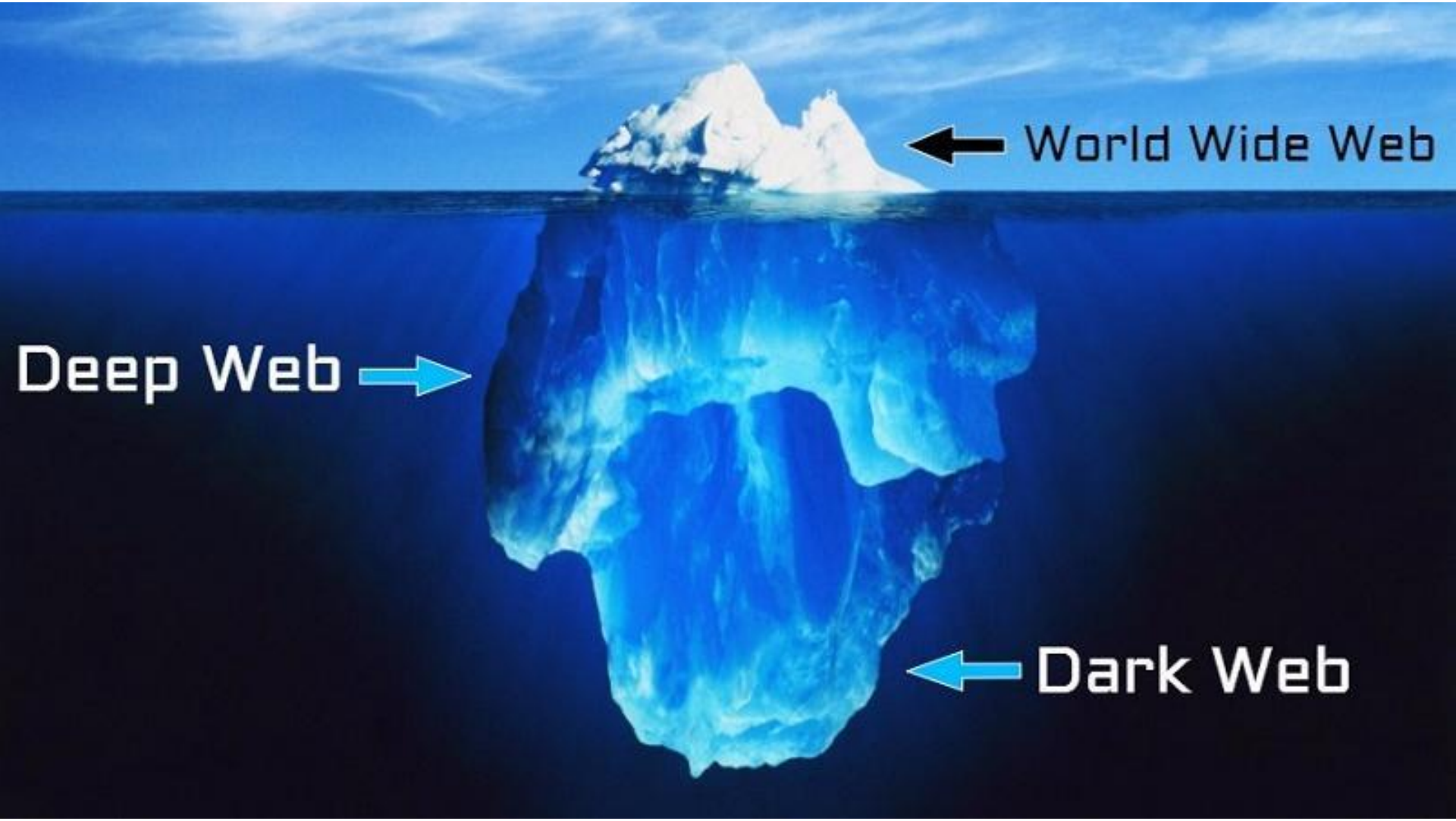
- Support the preparation, planning, coordination, and improvement of FSLTT agencies' resilient communications capabilities and operations
- Provide CISA with feedback and assessments of emergency communications across the nation
- Promote emergency communications at all levels of government
- Support state and territorial wide governance for emergency communications and help drive development and implementation of Statewide Communications Interoperability Plans
- Coordinate technical assistance, training, and exercise support

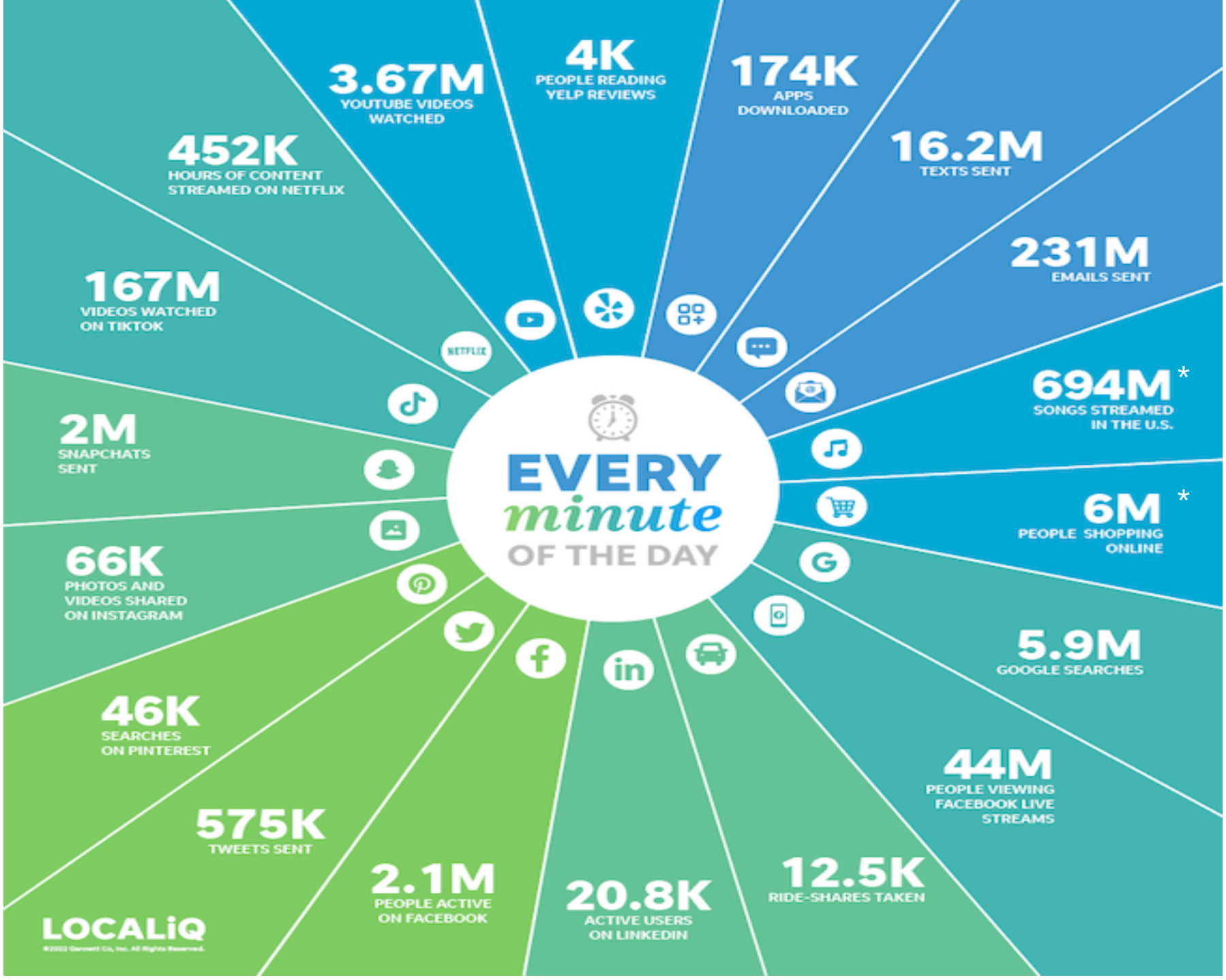


Common Cybersecurity Misconceptions

- I’m not important enough or big enough to be at risk of a cyberattack
- My devices are “secure enough” right out of the box
- Cybersecurity Problems are somebody else’s problems
- The human factor will always be a vulnerability

The Internet




EVERY
minute
OF THE DAY
3.67M
YOUTUBE VIDEOS WATCHED
4K
PEOPLE READING YELP REVIEWS
174K
APPS DOWNLOADED
16.2M
TEXTS SENT
231M
EMAILS SENT
694M*
SONGS STREAMED IN THE U.S.
6M*
PEOPLE SHOPPING ONLINE
5.9M
GOOGLE SEARCHES
44M
PEOPLE VIEWING FACEBOOK LIVE STREAMS
12.5K
RIDE-SHARES TAKEN
20.8K
ACTIVE USERS ON LINKEDIN
2.1M
PEOPLE ACTIVE ON FACEBOOK
575K
TWEETS SENT
46K
SEARCHES ON PINTEREST
66K
PHOTOS AND VIDEOS SHARED ON INSTAGRAM
2M
SNAPCHATS SENT
167M
VIDEOS WATCHED ON TIKTOK
452K
HOURS OF CONTENT STREAMED ON NETFLIX
LOCALiQ

What is Cybersecurity Risk?

Cyber Risk: The likelihood that any specific threat will exploit a specific vulnerability that causes harm as a result of the unauthorized disclosure, modification, or destruction of information or loss of information or system availability.

Threat

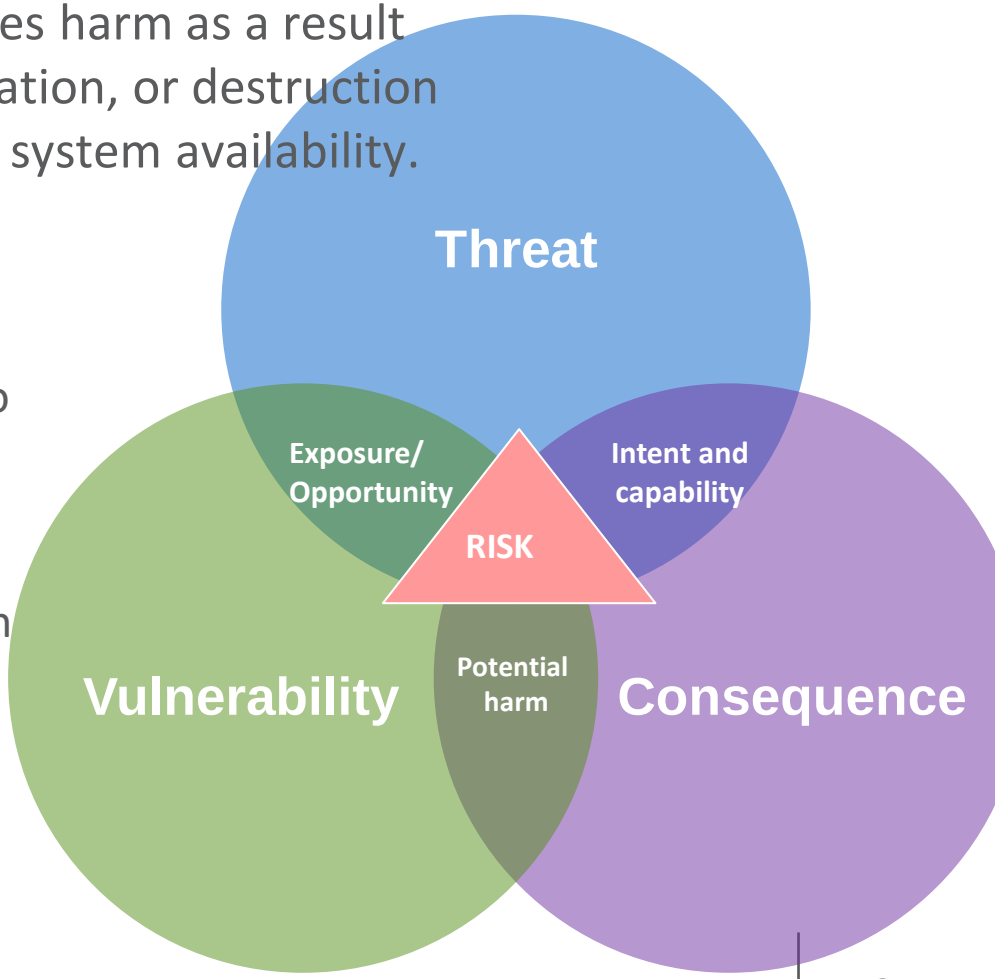
- People, programs, hardware, or systems with the intent, capability, and opportunity to exploit vulnerabilities

Vulnerability

- A weakness in the information (IT) or operational (OT) technology infrastructure or any other aspect of an organization.

Consequence

- Effect of an event, incident, or occurrence



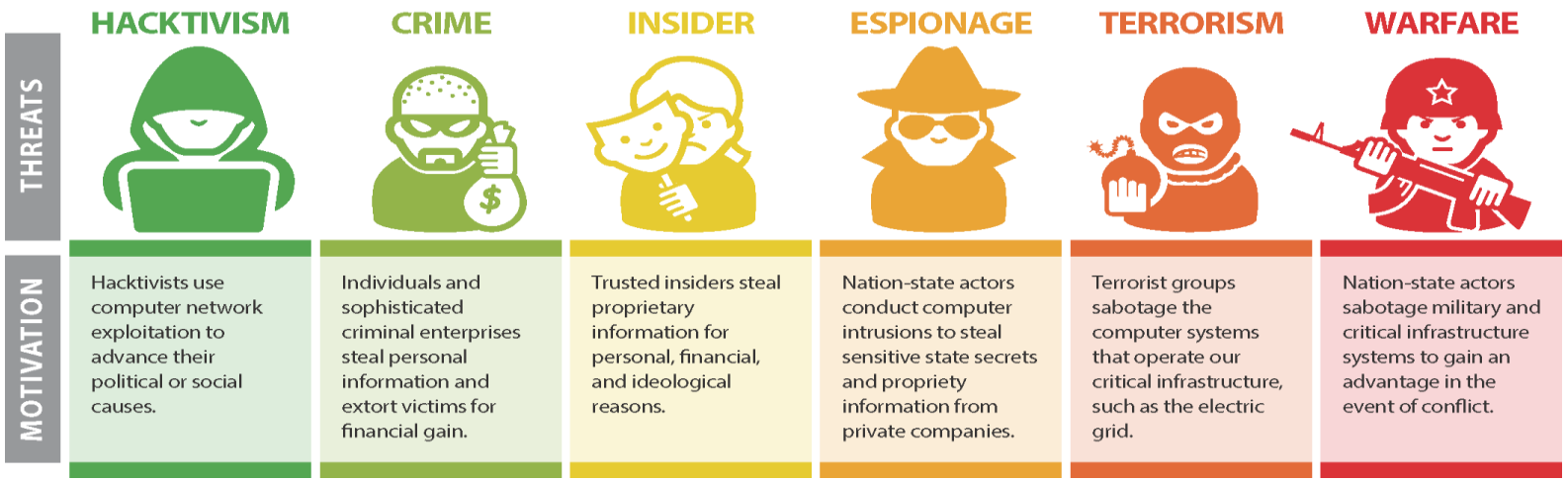
The Threat is Real

- Global cybercrime costs are expected to grow by 15% per year over the next five years, reaching $10.5 trillion annually by 2025.
- The entire cost of cyberattacks in 2022 was **$6 trillion**.
- **95%** of **data breaches** are the result of human error.
- Globally, **30,000 websites** are hacked daily.
  - **64% of companies** worldwide have experienced at least one form of cyber attack.
- There were **22 billion** breached records in 2021.
- In 2021, ransomware cases grew by **92.7%.**
- Email is responsible for around **94% of all malware**.
- **Every 39 seconds,** there is a new attack somewhere on the web.
- An average of **around 24,000 malicious mobile apps** are blocked daily on the internet.

https://techjury.net/blog/how-many-cyber-attacks-per-day/#gref

Threat Actors

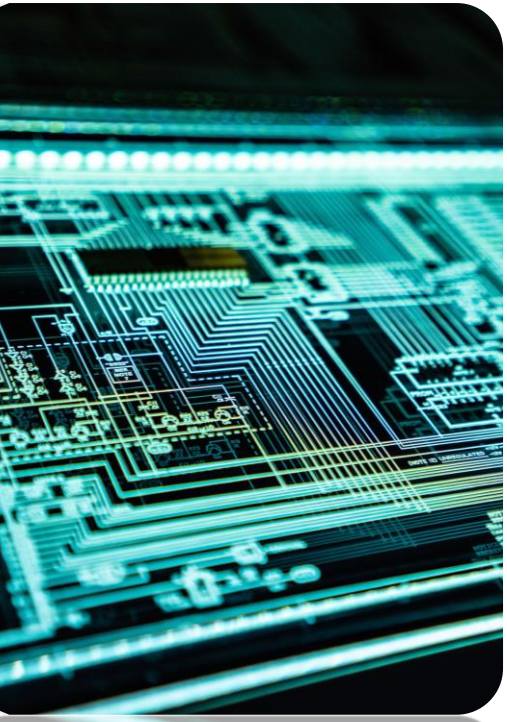
- "Outsiders"
  - Hackers (looking for financial gain)
  - Hacktivits (on ideological mission)
  - Organized crime groups
  - Terrorists
  - Competitors
  - Nation states
- "Insiders"
  - Current/former employees
  - Current/former service providers, consultants, contractors
  - Suppliers/customers
  - Business partners
  - Information brokers



Vulnerability and Opportunities for Compromise

- Social Engineering
  - Phishing Susceptibility
  - ‘Just trying to help’
- Exposed Software (Common Vulnerabilities and Exposures (CVEs))
  - Known Exploited Vulnerabilities
  - Vulnerabilities with Exploits Available
  - Critical and High Severity CVEs
- Prolonged windows of vulnerability exposure
- Exposed vulnerable services and protocols that can facilitate compromise (e.g., RDP)
- End of support and out of date operating systems and software

Consequences



Threat actors engage in targeted campaigns as well as indiscriminate vulnerability scanning for victims of opportunity to compromise IT and OT assets. Compromise of IT can indirectly affect or spread to OT if not contained.

2022 – North Korea-linked hacking campaign

- Using phishing emails sent from fake job recruiters targeted chemical companies in South Korea.

2021 – DarkSide Ransomware Campaign

- Three major international companies compromised
- One international company reportedly paid $4.4 million for 150GB of “sensitive data”
- Delays in productions and logistics and result in missed sales growth targets

2019 – LockerGoga Ransomware Campaign

- Affected two major US-based chemical companies
- Prevented access to IT systems and data and manufacturing was “not affected”
- Recovery involved ordering hundreds of new computers, and new email accounts

WORLDWIDE THREAT ASSESSMENT

Russia

Russia poses a cybersecurity threat to the United States and our allies. It is a highly capable and effective adversary, integrating cyber espionage, attack, and influence operations to achieve political and military objectives.

China

China presents a persistent cyber threat to our military and CI. It remains the most active strategic competitor responsible for cyber espionage against the U.S. Government, corporations, and allies.

Iran

Iran continues to present a cyber threat, using increasingly sophisticated techniques to conduct cyber espionage and deploy capabilities that would enable cyber attacks against CI in the United States.

North Korea

North Korea poses a cyber threat to financial institutions, remains a cyber espionage threat, and retains the ability to conduct disruptive cyber attacks.

Non-State Actors

Foreign cyber criminals, terrorists, and others will continue to conduct malicious cyber attacks to further their goals, aided by the growing availability and use of publicly available cyber tools.

Threat = Capability + Intent + Motivation

Election Threats: Misinformation Platforms

YouTube

LinkedIn

Google

facebook

twitter

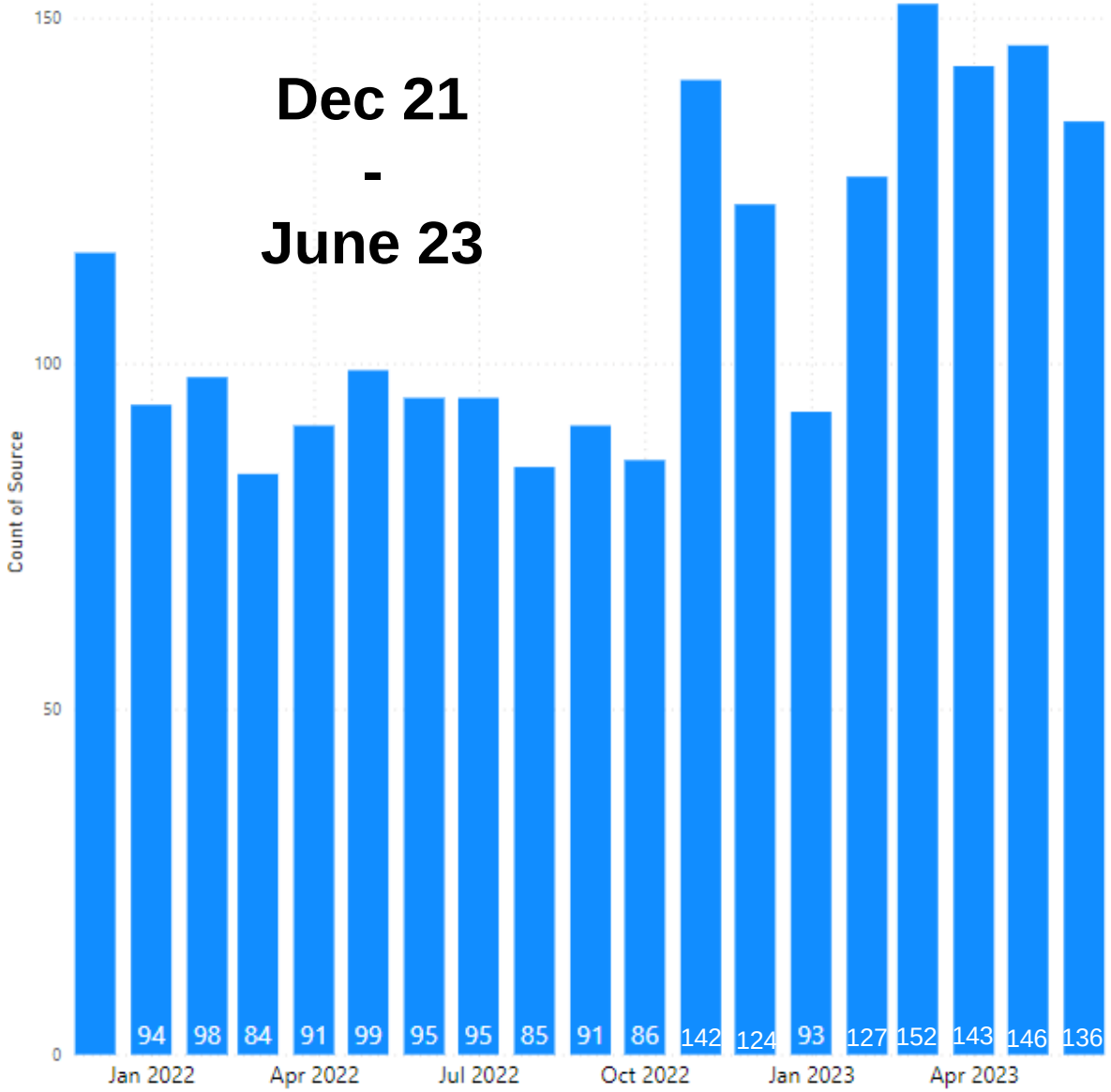
Gmail

Tik Tok

Public Enemy #1 Today: Ransomware

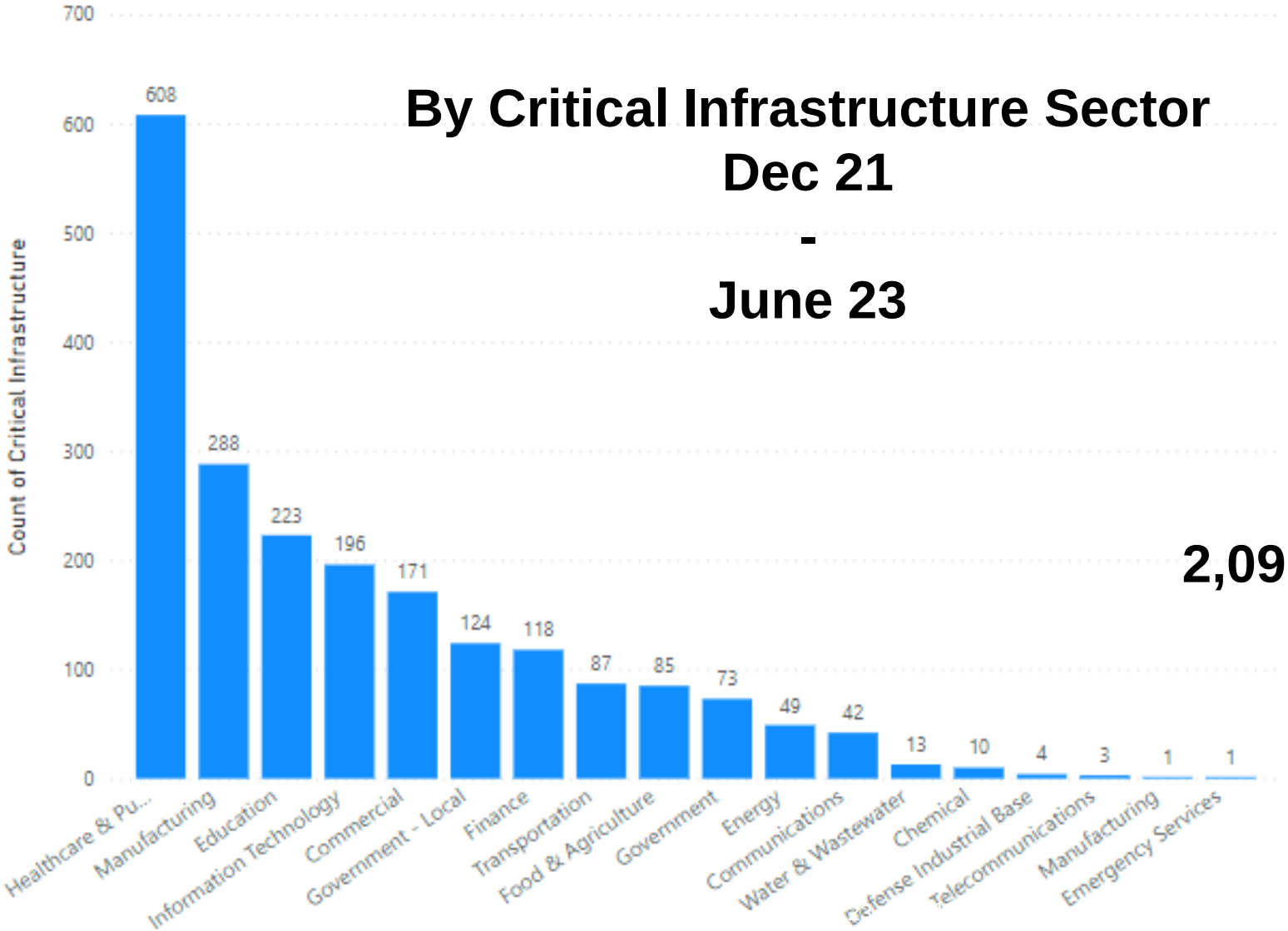
- **Ransomware**
  Malicious software that encrypts \ locks your data until a sum of money is paid (or a decryption key is found).

Ransomware Reported to CISA



2,097 Total

Ransomware Reported to CISA



2,097 Total

Notable Chemical Cyber Events

Companies say hacker activity caused temporary production shutdowns

Chemical distributor pays $4.4 million to DarkSide ransomware

The average cost of one cybersecurity incident in the industrial control system (ICS) and operational technology (OT) environment is $2,989,550.

Ponemon Institute's 2021 State of Industrial Cybersecurity

Lazarus group conducting cyber espionage against chemical sector, Symantec detects

APRIL 18, 2022

Cyber Incidents in South Dakota

(and neighboring states)

MINNEAPOLIS PUBLIC SCHOOLS
Urban Education. Global Citizens.

PayPal

DesMoines PUBLIC SCHOOLS

Phishing Assessments

1. External?

news@spdb.org

[EXT] Gubernatorial debate references state employees

[redacted]

Expires 10/01/2020

If there are problems with how this message is displayed, click here to view it in a web browser.

2. Were you expecting a message from this sender?

3. Compare name / alias to From: address

4. Don't fall for an emotional trap

Gubernatorial Candidates Debate Value of State Employees

From SPDB's Shawn Miller

(SPDB) - [Daily News, posted on Monday Oct. 1 10:13 p.m. CST]

A spirited debate was held Monday night on the campus of the University of South Dakota in Vermillion. In the historic Old Main building, candidates Congresswoman Kristi Noem and state Senator Billie Sutton debated a wide range of topics over two hours. In addition to the normal political topics of education, economic development and taxes, other subjects included the Keystone XL pipeline, state employees and water rights. For details on the comments made, please follow the story...

Read More

5. Hover over links

6. Report to the Help Desk

http://rg8bm90ignsawnrig9uihr
oaxmgbgluayeh.sd.gov.online/
?rid=x9wjk6o

Email Phishing Indicators

Email Phishing Indicators

Sender's email address mimics legitimate business
Generic greeting used –vs- your name
Lack of contact information within signature block
Email content misspelled your name
Email content contains poor grammar
Email content demands your urgent action
Email requests you to click an embedded hyperlink
Email requests you to read a suspicious file attachment

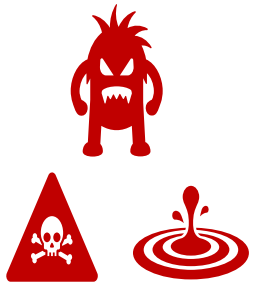
Your Actions:

- Confirm true destination of URL before clicking
- Manually visit the alleged sender's website
- Scan the file attachment for malware before opening
- **Notify your security/CI office of the email; they will require the original email so don't delete it**

A More Proactive, Less Reactive Approach

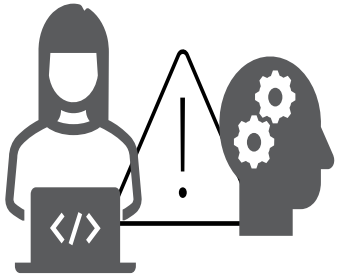
Leverage known threat and consequence information to proactively identify vulnerability exposure among entities and sectors that support national critical functions and provide vulnerability and risk intelligence that enables action to reduce cybersecurity risk.

BE AWARE OF



KNOWN THREATS
AND CONSEQUENCES

IDENTIFY AND ANALYZE

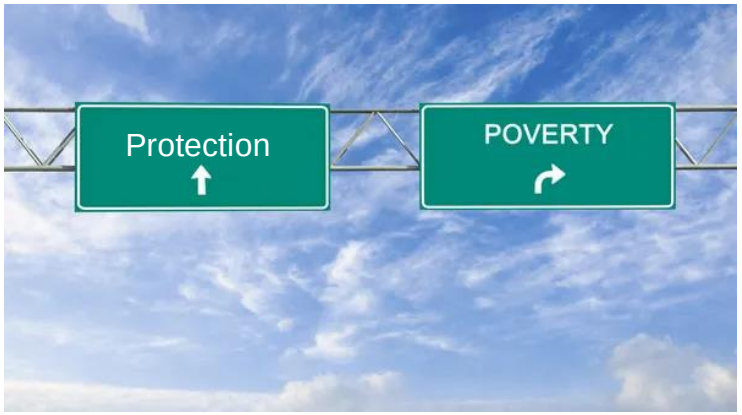


KNOWN IT AND OT
VULNERABIITY EXPOSURE

TAKE ACTION

REDUCE CYBERSECURITY RISK

Best Practices in Cybersecurity Hygiene



A. Business Priorities
B. Cybersecurity Training
C. Inventory
D. Passwords
E. Identity Management
F. Network Segmentation
G. Vulnerability Management
H. Outside Support
I. Vendor Management
J. DR & Incident Response
K. Threat Detection
L. Security Policy
M. External / 3rd Party Assessments

CISA Cyber Stakeholder Services

Strategic Risk Assessments
(Field Driven)

- Cyber Resilience Review (CRR)
- External Dependencies Management (EDM)
- Cyber Resilience Essentials (CRE)
- Cyber Performance Goals (CPG)
- Cyber Incident Management Review (IMR)
- Cyber Protective Visit (CPV)
- Cyber Infrastructure Survey (CIS)

Workshops
(Field Driven)

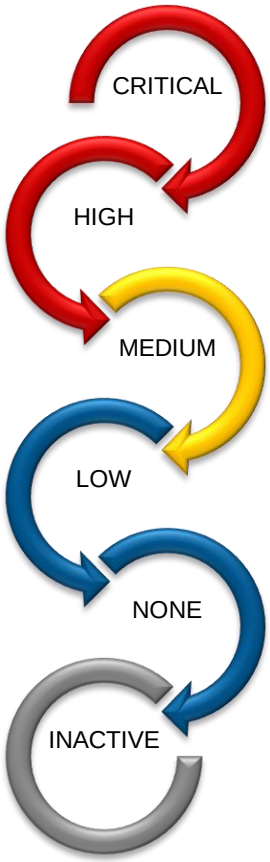
FREE

- Cyber Resilience
- Incident Management
- Critical Functions
- SLTT
- Vulnerability Management
- External Dependencies

Vulnerability Scanning - Technical

FREE

Vulnerability Port Scanning Service



- Automated scanning of Internet / External accessible systems (Top 1000 Ports / NMAP & Nessus) (could include some cloud sites)
- ICMP, Ping, Open, Ports
- Helps individual customer understand their exposure
- Informs national risk management efforts
- Weekly report card that include current scan results, historic trends, and result comparisons to the national average
- Federal agencies must mitigate critical vulnerabilities within 15 or 30 days of detection (Critical vs High)
- 2-4 weeks wait time to get request processed
- Unlimited capacity of subscribers

CISA
CYBER+INFRASTRUCTURE

Are you Above or Below the Cybersecurity Poverty Line?

CISA Web Resources of Interest

- https://www.cisa.gov/
- https://www.cisa.gov/**shields-up**
- https://www.cisa.gov/**stopransomware**
- https://www.cisa.gov/**cyber-essentials**
- https://www.cisa.gov/**cyber-resource-hub**
- https://www.cisa.gov/uscert/ncas/**alerts/2023**
- https://www.cisa.gov/**known-exploited-vulnerabilities-catalog**
- https://www.cisa.gov/resources-tools/services/**cisa-tabletop-exercise-packages**
- https://github.com/cisagov
- https://fedvte.usalearning.gov/
- https://ics-cert-training.inl.gov
- https://www.usajobs.gov/

CISA
CYBER+INFRASTRUCTURE

Incident Reporting Contacts

Threat Response	Asset Response
Federal Bureau of Investigation 855-292-3937 or cywatch@ic.fbi.gov	**CISA Central** 888-282-0870 or central@cisa.DHS.gov Report suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to further improve security.
U.S. Secret Service secretservice.gov/contact/field-offices **SD Fusion Center** 1-866-466-5263 https://fusion.sd.gov/	
Immigration and Customs **Homeland Security Investigations** 866-347-2423 or ice.gov/contact/hsi	**Report Internet Crimes**: FBI Internet Crime Complaint Center ic3.gov

CISA
CYBER+INFRASTRUCTURE

Message Takeaways

Prioritize Cybersecurity

Recognize the Risk

Free CISA Resources

Proactive wins over Reactive

SD CISA Resources

Jim Edman Cybersecurity Coordinator	Jim.Edman@cisa.dhs.gov 605.220.1567
Shane Hoenke Cybersecurity Advisor	Shane.Hoenke@cisa.dhs.gov 605.381.6648
Scott Davis Supervisory Protective Security Advisor	Scott.L.Davis@hq.dhs.gov 605.224.1291
Brad Eggers Protective Security Advisor	Bradley.Eggers@cisa.dhs.gov 605.209.0022
Thad Fitch Chemical Security Inspector	Thad.Fitch@hq.dhs.gov 202.302.6363
Jeremy Johnson Telecommunications Specialist	Jeremy.Johnson@cisa.dhs.gov 202.431.8962