CISA | CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY

Jeremy Bullock
SAFE SCHOOLS SUMMIT

WHEN DOORS AND DATA COLLIDE: UNDERSTANDING HOW CYBER THREATS IMPACT PHYSICAL SECURITY

Albert Mendoza, Protective Security Advisor

Joe Frohlich, Cybersecurity Coordinator

CYBERSECURITY &
INFRASTRUCTURE
SECURITY AGENCY

Mission

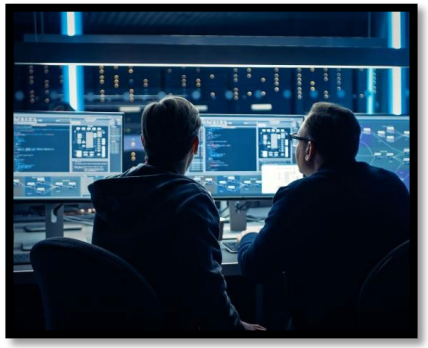
We lead the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.

Vision

A secure and resilient critical infrastructure for the American people.

Who We Are:

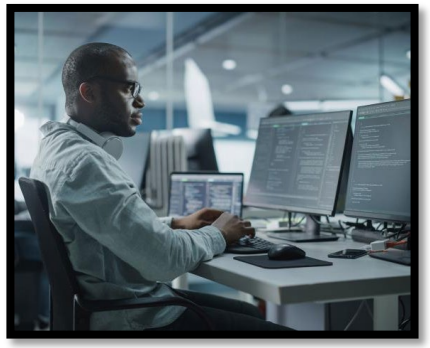
CISA consists of



Cybersecurity

Infrastructure Security

Emergency Communications

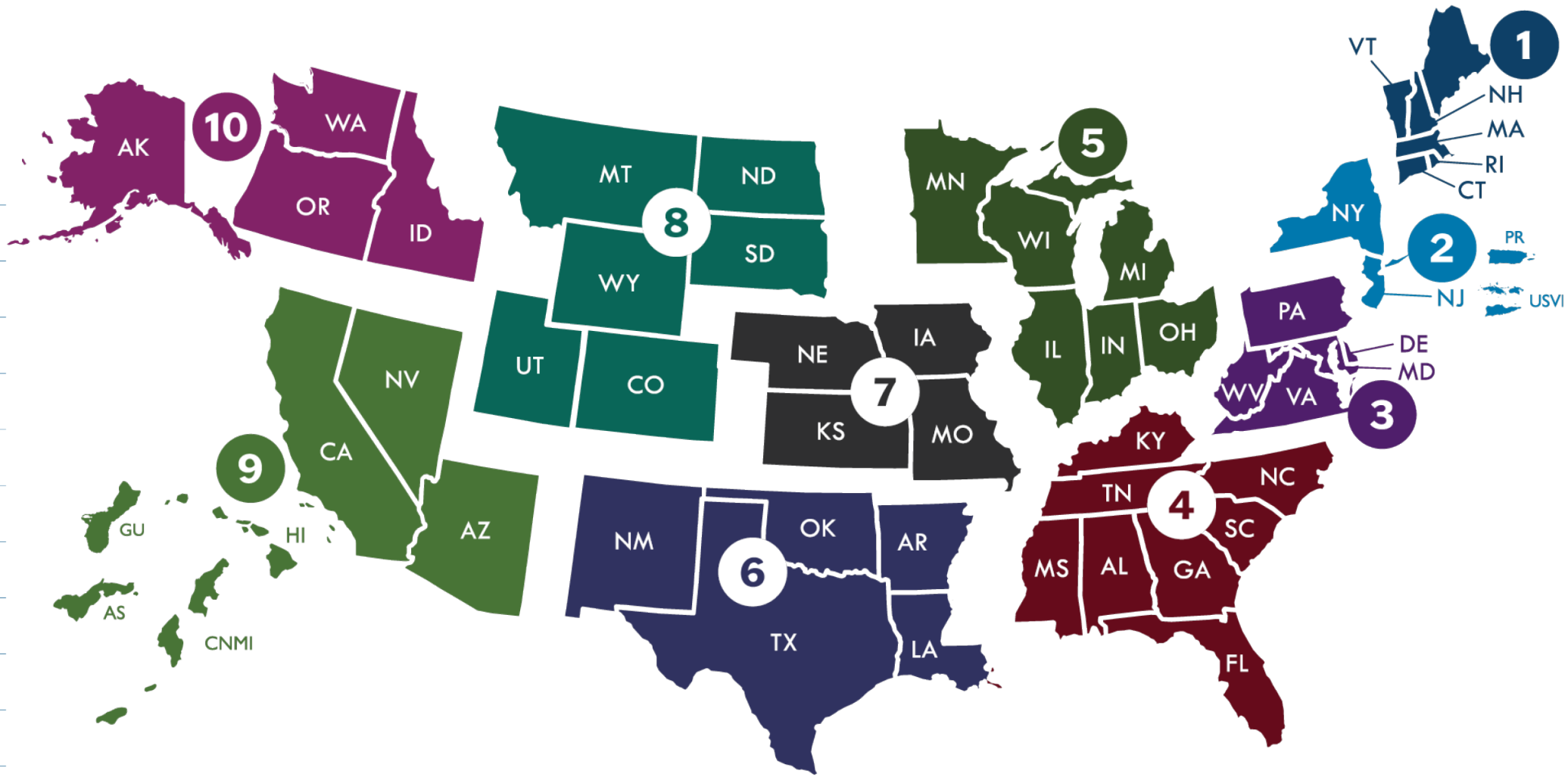


National Risk Management Center

CISA works with public sector, private sector, and government partners to share information, build greater trust, and lead the national effort to protect and enhance the resilience of the Nation's physical and cyber infrastructure.

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



CISA.GOV/REGIONS

16 Sectors & Sector Specific Agencies

→ 2025 CISA Priority Sectors ←

CISA Region 8 – Montana Cadre

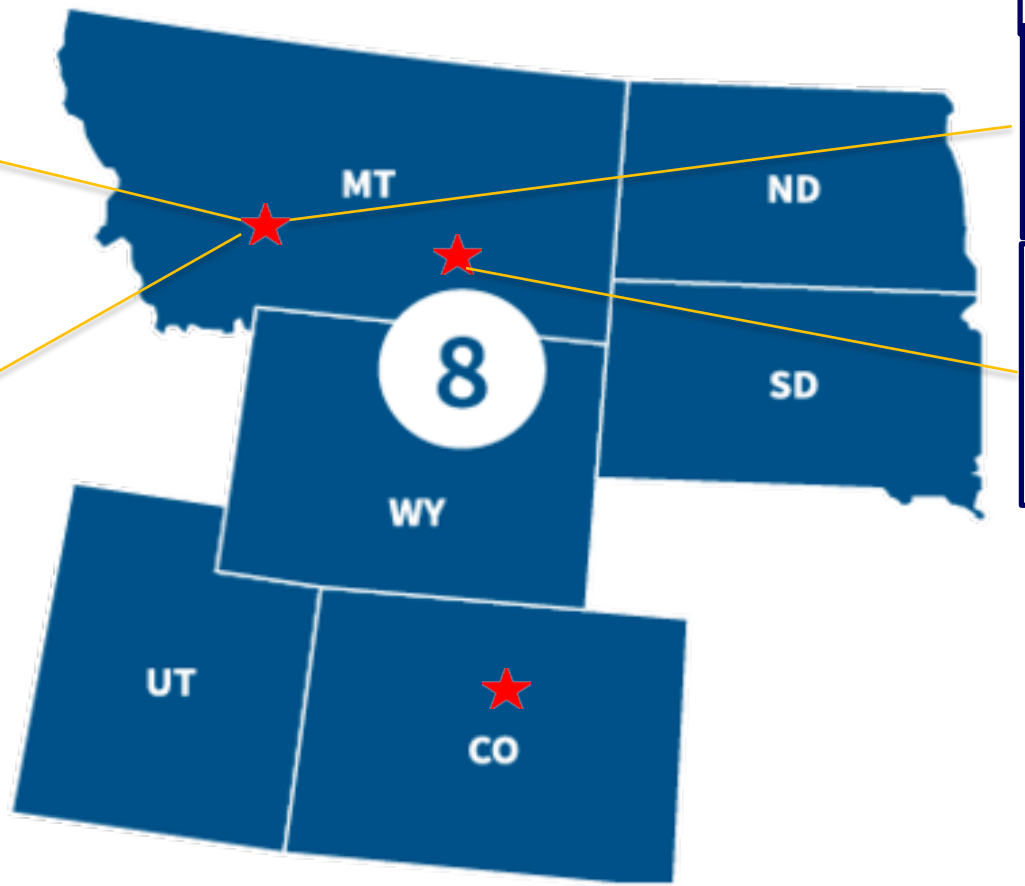
CISA
Cyber Security Advisors

Joe Frohlich

Cybersecurity State Coordinator (CSC)
State & Local Government,
K-12, Higher Education
Helena

Travis Light

Cybersecurity Advisor (CSA)
Critical Infrastructure Focus
Helena



CISA
Protective Security Advisors

Randy Middlebrook

Protective Security Advisor (PSA)
Helena

Albert Mendoza

Protective Security Advisor (PSA)
Billings

Protective Security Advisor (PSA)

- **INFRASTRUCTURE SURVEY TOOL** - Identifying facilities' physical security, security forces, security management, information sharing, protective measures, and dependencies related to preparedness, mitigation, response, resilience, and recovery;

- **Assist Visit** – Identifies and recommends protective measures at facilities, provide comparison across like assets, and track implementation of new protective measures.

- **Infrastructure Visualization Platform (IVP) –** brings a facility's digital floorplans to life by placing on it 360° panoramic photographs, immersive video, geospatial information, and hypermedia data of critical facilities, surrounding areas, and transportation routes that assist with security planning, protection, and response efforts.

- **SAFE Tool** The Security Assessment at First Entry (SAFE) tool is designed to assess the current security posture and identify options for facility owners and operators to mitigate relevant threats

CISA Protective Security Advisors

Key Themes

1. Each school is unique; there is no one size-fits all approach to physical security.

2. Taking a systems-based approach to physical security can help schools address their unique circumstance and ensure that protection and mitigation measures complement measures to the prevent violence and respond to and recover from violent incidents.

3. Taking a layered approach to physical security ensures that the system works in an integrated way to Detect, Delay and Respond to threats and helps to prevent single points of failure.

Physical Security Overview

- Physical Security ,Equipment and Technology.

  Locks, card readers, camera system

- School Security Personnel.
- School Resource Officer? Dedicated security staff?
- Security Policies and Procedures.
- Are there policies and procedures in place to inform members of the school community (staff, students, visitors, etc.) of actions they should take in case of an emergency

Physical Security Overview

- Site and Building Design.
- Where is the school located? Is it in rural, suburban, or urban locale? How long does it take first responders such as police and emergency medical services to reach the school in an emergency?
- Training, Exercise and Drills.
- What type of training is conducted and how often? Active shooter, De-escalation, are local first responders included?

Cyber Risk

Cybersecurity is everyone's responsibility

Peoples Republic of China (PRC) Cyber Threats

- “While the PRC is a sophisticated cyber adversary, many of its methods to break into our critical infrastructure are not. They don’t have to be. Why? Because we’ve made it easy for them. The truth is that, in many cases, the PRC is taking advantage of known product defects.”

- CISA Director Jen Easterly
(January 31st, 2024 - Opening Statement before the House Select Committee)

Office of Intelligence and Analysis – Feb 2025

OFFICE of INTELLIGENCE and ANALYSIS
INTELLIGENCE IN FOCUS

CYBERSECURITY

(U//FOUO) **People's Republic of China: Exploitation of Internet-Connected Cameras Threatens US Critical Infrastructure**

(U//FOUO) **The ability of People's Republic of China (PRC) cyber actors to access internet-connected cameras—especially those manufactured in the PRC—in the Homeland probably enables Beijing to conduct espionage or disrupt US critical infrastructure.**[a] These devices typically lack data encryption and security settings and have default settings to communicate with their manufacturer, which, for PRC-made cameras, could be in China. There are tens of thousands of PRC-made cameras on the

Verkada - Surveillance Camera Security Breach – March 2021

The hackers responsible for the breach claimed that they were able to access Verkada's systems by exploiting a "Super Admin" account that had been left unprotected. Once inside, they were able to view live feeds from cameras installed in a wide range of locations, including offices, factories, hospitals, prisons, and schools. The hackers also gained access to archived footage, which could potentially contain sensitive or incriminating information.

150,000 Surveillance Cameras Exposed in Verkada Security Breach - UMA Technology

https://www.verkada.com/security-update/report/

Cloud Provider & Ransomware Breach's

IMAGE: ANNIE SPRATT VIA UNSPLASH/POWERSCHOOL

Suzanne Smalley
May 21st, 2025

Cybercrime News

College student to plead guilty to Power hack

https://therecord.media/college-student-to-plead-guilty-to-powerschool-hack

PowerSchool hacker now extorting individual school districts

By Lawrence Abrams — May 7, 2025 02:25 PM 0

https://www.bleepingcomputer.com/news/security/powerschool-hacker-now-extorting-individual-school-districts/

PRIVACY & SECURITY

Schools Are a Top Target of Ransomware Attacks, and It's Getting Worse

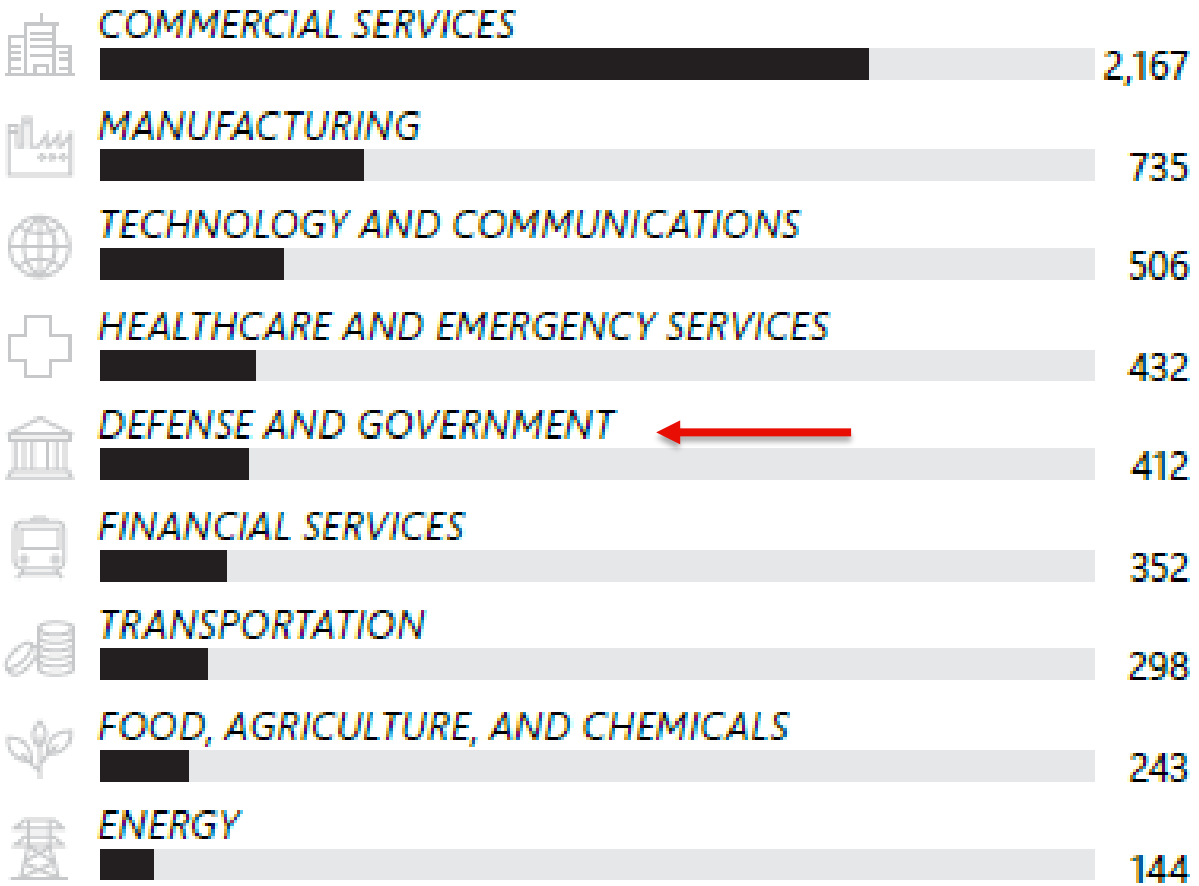
By Lauraine Langreo — August 17, 2023 3 min read

https://www.edweek.org/technology/schools-are-a-top-target-of-ransomware-attacks-and-its-getting-worse/2023/08

Ransomware Attacks by Industry (ODNI 2024)

TOTAL RANSOMWARE ATTACKS WORLDWIDE, BY INDUSTRY, 2024

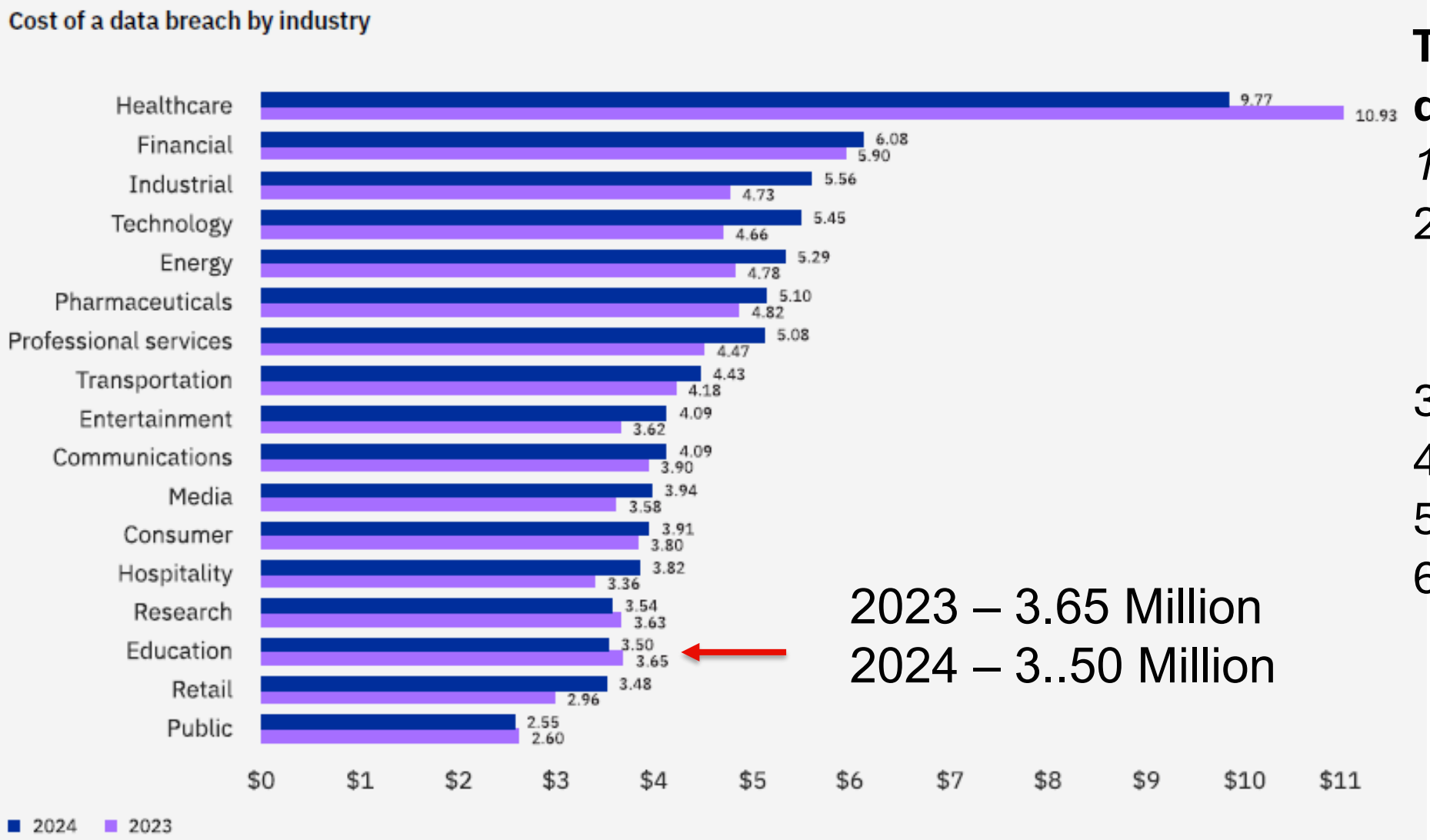
Commercial Services, Manufacturing, and Technology and Communications remained the most heavily targeted industries. Attacks against critical infrastructure pose an outsized threat to national security based on the potential for these attacks to disrupt essential services and critical functions.



TOTAL RANSOMWARE ATTACKS per YEAR (Worldwide)

2022	**2,593**
2023	**4,591 (77%↑)**
2024	**5,289 (15%↑)**

Cost of a Data Breach by Industry (IBM 2024)



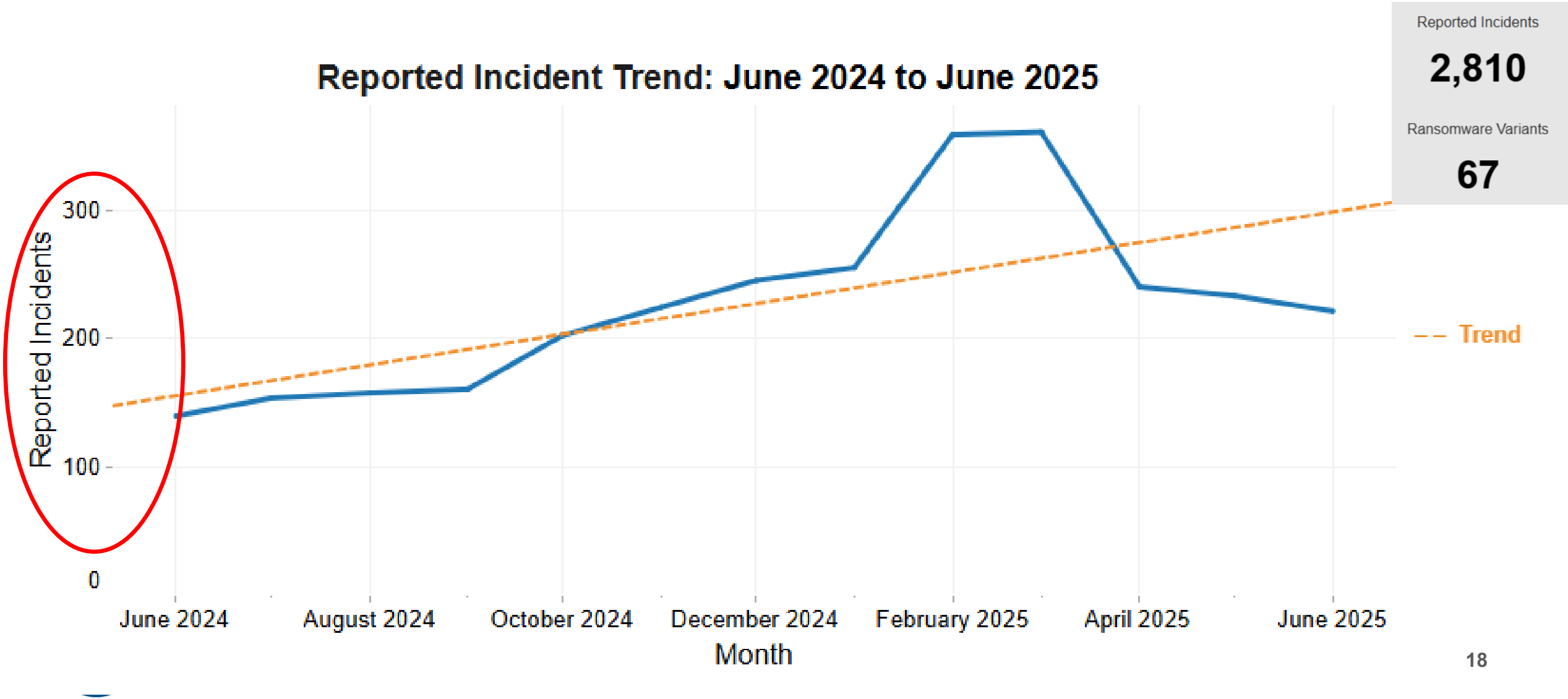
2023 – 3.65 Million
2024 – 3..50 Million

Top Factors to drive down breach cost:

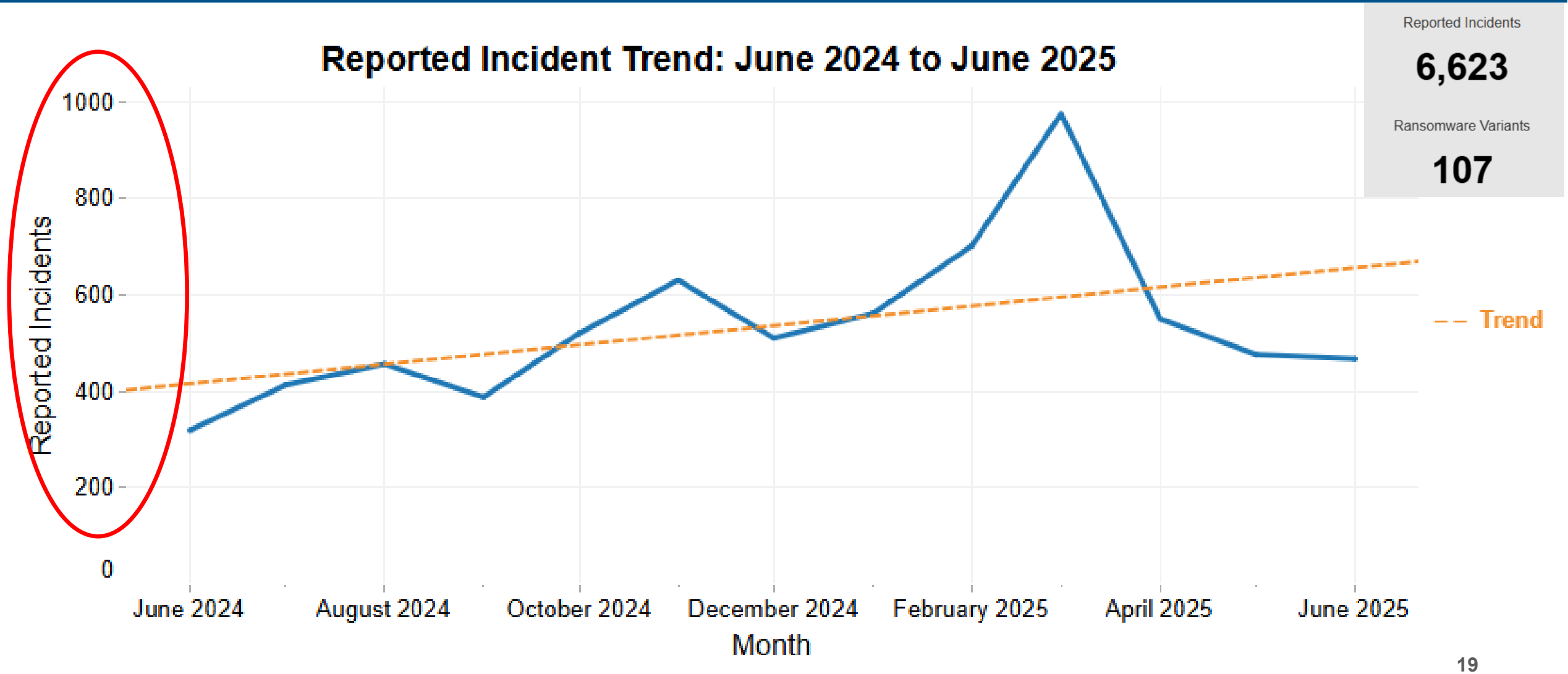
1. *Employee Training*
2. AI, machine learning driven insights
3. SIEM
4. IRP
5. Encryption
6. Threat Intel

if you SEE something | SAY something®

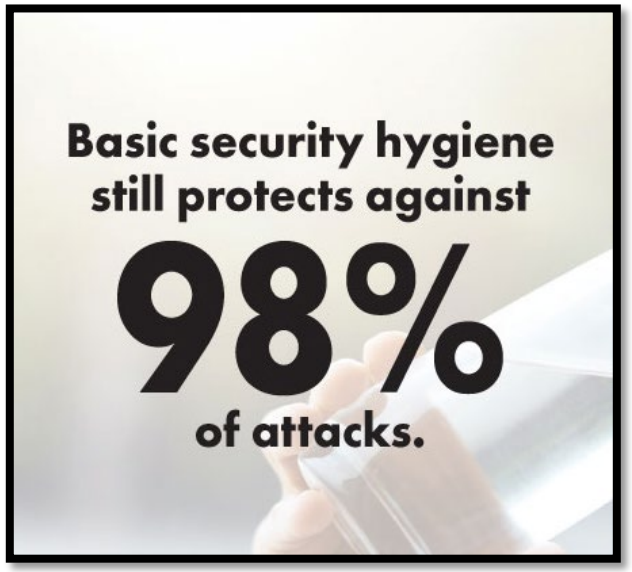
Ransomware Incidents: Reported to Federal Government



Ransomware Incidents: Dark Web Data



Attacks are Preventable



Basic Cyber Hygiene

Less than **25%** surveyed performed annual cybersecurity risk assessments.

Perform Risk Assessments

Enable MFA on Accounts

EPA OFFICE OF GROUND WATER AND DRINKING WATER

Statistics provided by EPA and FBI

CISA Cyber Services

Cybersecurity Advisor Program

Cybersecurity Advisors & Coordinators (CSAs / CSCs)
support CISA's Cybersecurity Mission in the following areas:

Specifically, what we do:

- **Perform Strategic Assessments**
- **Promote Technical Service Offerings**
- **Deliver Presentations**
- **Fulfill Entity Notifications**
- **Participate in Working Groups**
- **Offer Trainings**
- **Furnish CISA & Industry Information**
- **Conduct Topic Briefings**

Recommended CISA Cyber Assessments for Montana

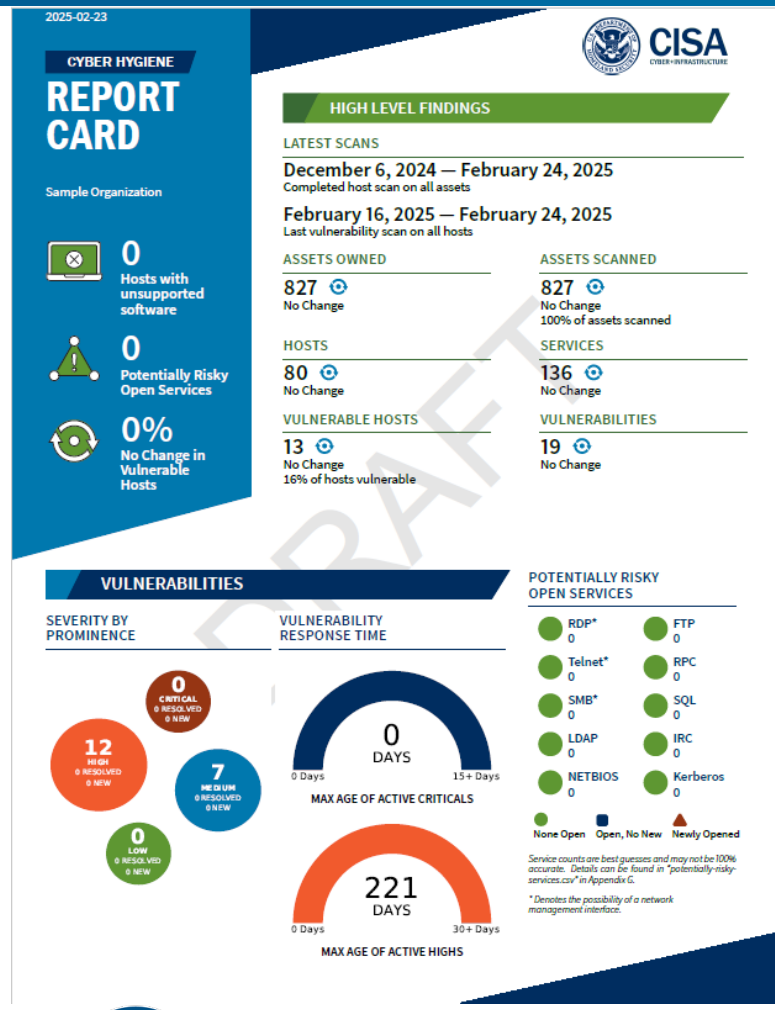
Cyber Resilience Essentials (Strategic) ----------
Cyber Performance Goals (Strategic) ----------
External Dependencies Management (Strategic) ----------

Vulnerability Scanning / Hygiene (Technical) ----------

To be eligible for additional technical assessments – Need to have

CISA Cyber Assessment & Vuln scanning in place

CISA Vulnerability Scanning – Report



2025-02-23

CYBER HYGIENE

REPORT CARD

Sample Organization

0 Hosts with unsupported software

0 Potentially Risky Open Services

0% No Change in Vulnerable Hosts

CISA

HIGH LEVEL FINDINGS

LATEST SCANS

December 6, 2024 — February 24, 2025
Completed host scan on all assets

February 16, 2025 — February 24, 2025
Last vulnerability scan on all hosts

ASSETS OWNED
827
No Change

ASSETS SCANNED
827
No Change
100% of assets scanned

HOSTS
80
No Change

SERVICES
136
No Change

VULNERABLE HOSTS
13
No Change
16% of hosts vulnerable

VULNERABILITIES
19
No Change

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL 0 RESOLVED 0 NEW
12 HIGH 0 RESOLVED 0 NEW
7 MEDIUM 0 RESOLVED 0 NEW
0 LOW 0 RESOLVED 0 NEW

VULNERABILITY RESPONSE TIME

0 DAYS
0 Days — 15+ Days
MAX AGE OF ACTIVE CRITICALS

221 DAYS
0 Days — 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0
FTP 0
Telnet* 0
RPC 0
SMB* 0
SQL 0
LDAP 0
IRC 0
NETBIOS 0
Kerberos 0

None Open — Open, No New — Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

* Denotes the possibility of a network management interface.

VULNERABILITIES

SEVERITY BY PROMINENCE

0 CRITICAL 0 RESOLVED 0 NEW

12 HIGH 0 RESOLVED 0 NEW

7 MEDIUM 0 RESOLVED 0 NEW

0 LOW 0 RESOLVED 0 NEW

VULNERABILITY RESPONSE TIME

0 DAYS
0 Days — 15+ Days
MAX AGE OF ACTIVE CRITICALS

221 DAYS
0 Days — 30+ Days
MAX AGE OF ACTIVE HIGHS

POTENTIALLY RISKY OPEN SERVICES

RDP* 0
FTP 0
Telnet* 0
RPC 0
SMB* 0
SQL 0
LDAP 0
IRC 0
NETBIOS 0
Kerberos 0

None Open — Open, No New — Newly Opened

Service counts are best guesses and may not be 100% accurate. Details can be found in "potentially-risky-services.csv" in Appendix G.

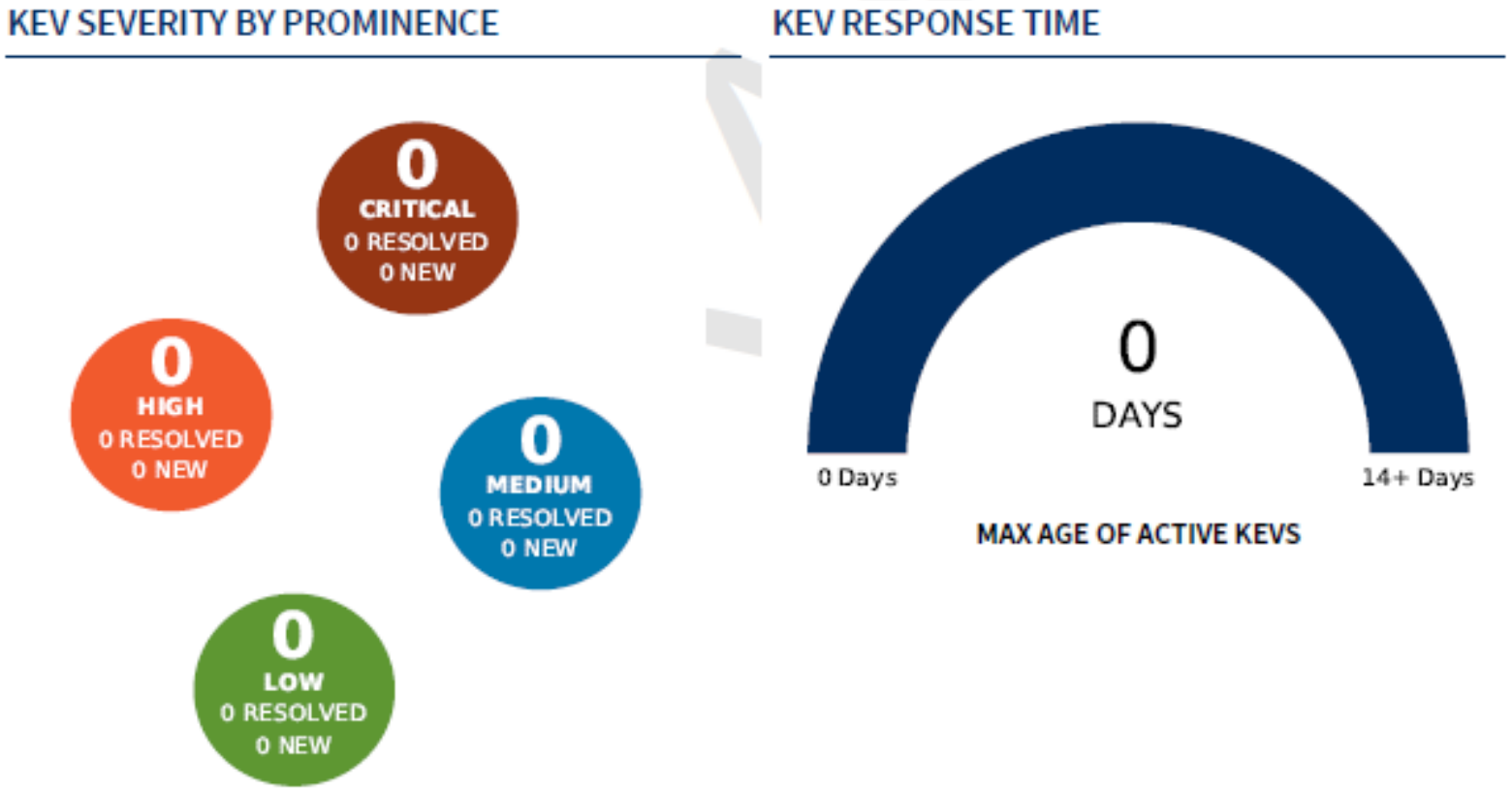
** Denotes the possibility of a network management interface.*

Page 6 of Vulnerability Scanning Report Review this page at least quarterly and have IT provide an update and remediation plan.

[Sign up - Cyber Hygiene Services]

CISA Vulnerability Scanning – Summary

Reducing the Significant Risk of Known Exploited Vulnerabilities (KEV)



Page 7 of Vulnerability Scanning Report Review this page at least quarterly and have IT give an update and remediation plan.

Sign up - Cyber Hygiene Services

Executive Summary page 6-11 on report

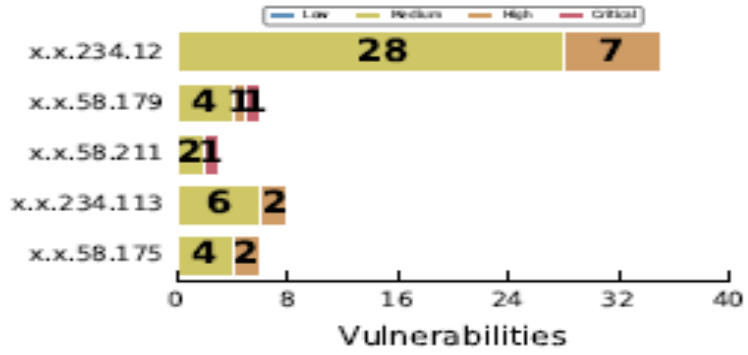


Figure 2: Top High-Risk Hosts

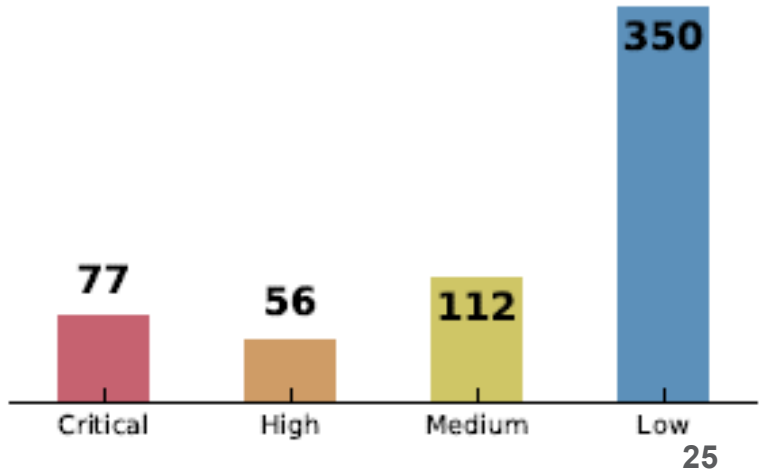


Figure 4: Median Time in Days to Mitigate Vulnerabilities

Incident Response Plans

[Insert Organization] Incident Response Plan

[Remove and insert your organizations logo]

[CISA Cybersecurity Incident Response Plan Basic Templates (Version 2025-04)]

Version: 2025-06-13

[Insert Organization] Cybersecurity Incident Response Plan

[Remove and insert your organizations logo]

[CISA Cybersecurity Incident Response Plan for Small Organizations. Guidance, Templates and Playbooks (Version 2025-04)]

Version: 2025-06-13

Incident Reporting

Montana Analysis and Technical Information Center (MATIC):

406-444-1330 | dojintel@mt.gov

CISA Central 24x7 contact number:

844-Say-CISA | SayCISA@cisa.dhs.gov

Report an Incident: www.cisa.gov/forms/report

State & Local Cyber Grant Program (K-12 included)

Applications will be completed through MT DES - des.mt.gov

Committee Approved Projects for Montana's K-12

- End User Security Awareness Training (Staff)
  - KnowBe4 Diamond Tier though the State of Montana Contract
- ★ Behavior Based Endpoint Protection (Server and Workstation)
  - Sentinelone - $63 per workstation, $90 per server – though State of Montana Contract
- ★ Professional Cybersecurity Training (for IT Privileged users and Cyber Professionals)
  - Up to $4,500

SecureMontana – Whole of State Cyber/Physical Security

Next Meeting is August 28th – 1PM to 3PM

- In Person (Missoula, MT – Hosted by University of Montana)

- Join SecureMontana's Discord Channel
  - https://discord.gg/Shg7f4SYwj
    - Chat with SecureMontana members
    - See upcoming meeting information
    - See/Post upcoming Montana Training and conferences… and so much more.

- Current Website – www.Cyber406.org

CISA School Safety & Cybersecurity for K-12

School Safety

- K-12 Bystander Reporting Toolkit
- SchoolSafety.gov
- K-12 School Security Guide Product Suite

Cybersecurity for K-12

- Cyber Education Resources
  - K-5, 6-8, 9-12
- STOP Ransomware (K-12)
- Cybersecurity Guidance for K-12 Technology Acquisitions

Any Questions or Comments?

CISA Contact Information

Joe Frohlich Cybersecurity State Coordinator Region 8 - Montana	joseph.frohlich@mail.cisa.dhs.gov 406-461-2651
Travis Light Cybersecurity Advisor Region 8 - Montana	travis.light@mail.cisa.dhs.gov 406-894-8374
Randy Middlebrook Protective Security Advisor Region 8 - Montana	randy.middlebrook@mail.cisa.dhs.gov 406-839-1165
Albert Mendoza Protective Security Advisor Region 8 - Montana	albert.mendoza@mail.cisa.dhs.gov 406-371-3585

Jeremy Bullock
SAFE SCHOOLS SUMMIT