AVAILABLE CISA SERVICES TO AID IN MITIGATING FINANCIAL SECTOR DATA BREACHES

Region IV (South Carolina)

Columbia Area

Protective Security Advisor (PSA)
- Keith Jones

Cybersecurity State Coordinator (CSC)
- CL Clay

Charleston / Mt. Pleasant Area

Protective Security Advisor (PSA)
- Amanda Knight

Cybersecurity Advisor (CSA)
- Anthony E. Carbone

11 October 2024

Agenda

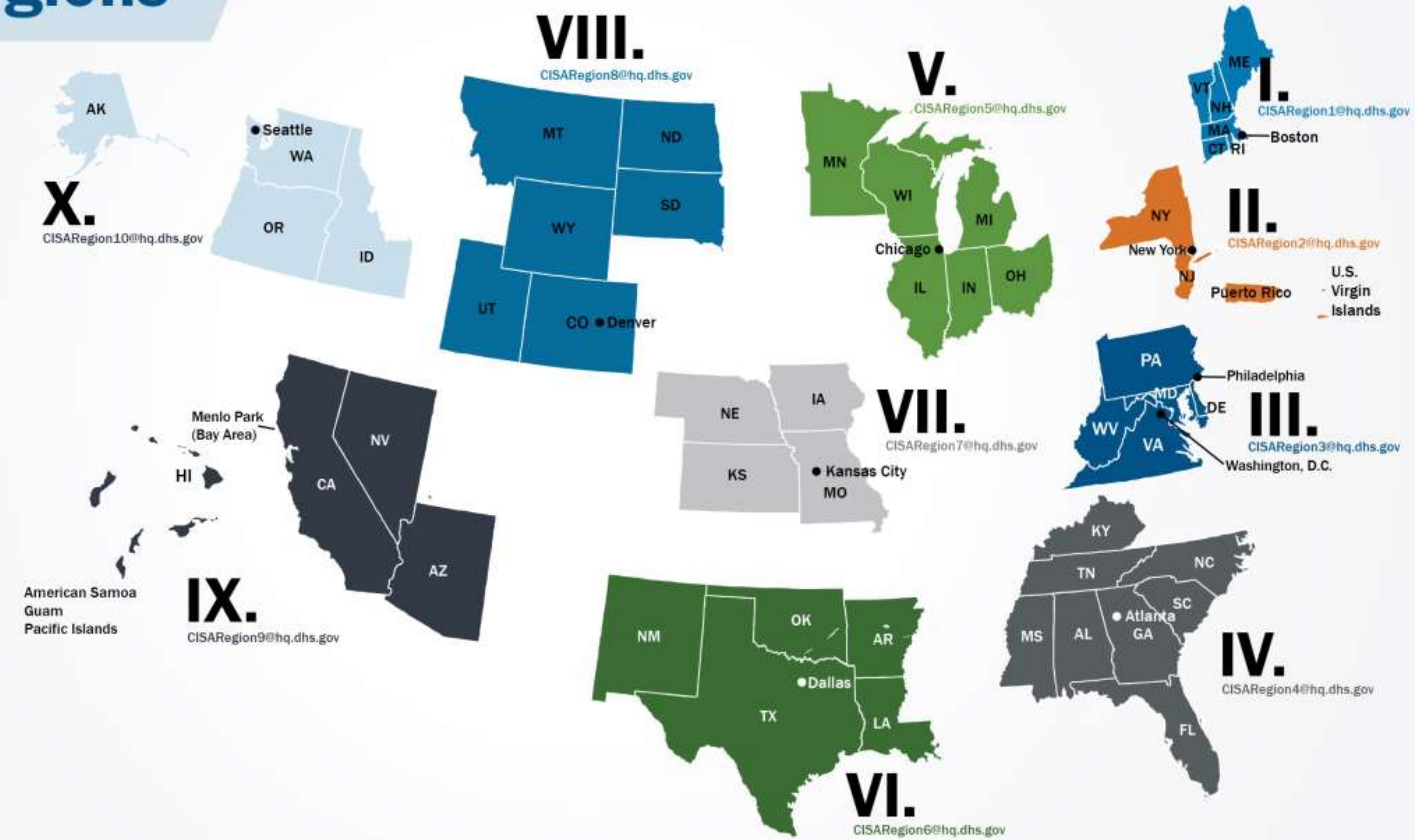
- CISA Introduction and Mission
- CSA/CSC & PSA Programs
- Current Data Breach Landscape
- Understanding & Managing Risk
- What Can You Do & How CISA Can Help
- Q & A

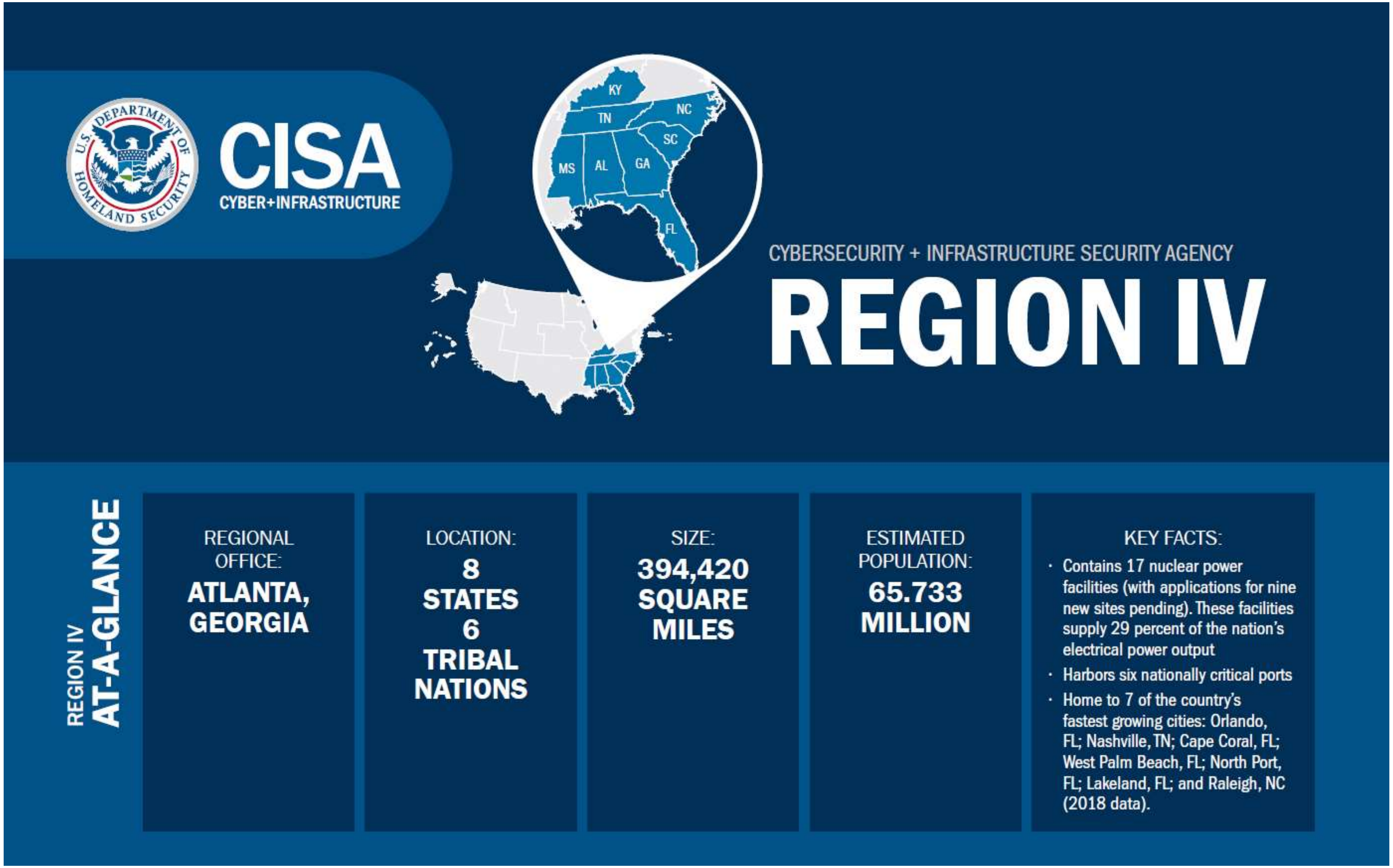
WHO WE ARE

INTRODUCTION & MISSION

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




KY
TN
NC
SC
MS
AL
GA
FL

CISA CYBER+INFRASTRUCTURE

CYBERSECURITY + INFRASTRUCTURE SECURITY AGENCY

REGION IV

REGION IV **AT-A-GLANCE**

REGIONAL OFFICE:	LOCATION:	SIZE:	ESTIMATED POPULATION:	KEY FACTS:
ATLANTA, GEORGIA	**8 STATES 6 TRIBAL NATIONS**	**394,420 SQUARE MILES**	**65.733 MILLION**	· 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).

Learn More About The CISA Integrated Operations Division (IOD) And Its Mission at: Infrastructure Security Division | Cybersecurity and Infrastructure Security Agency CISA

CYBERSECURITY STATE COORDINATOR (CSC) / CYBERSECURITY ADVISOR (CSA) PROGRAM

CSC / CSA Program

Program Established in Section 2215 of the 2021 National Defense Authorization Act

Cybersecurity State Coordinators (CSCs) are highly qualified CISA employees appointed to **serve in each state as the principal point of contact** with CISA on preparing, managing, and responding to cybersecurity risks and incidents.

Post 2021 NDAA: Cybersecurity Advisors (CSAs) subsequently hired for each state to further support CISA's cybersecurity program with emphasis on Critical Infrastructure (CI) Support.

What Do We Do?

- **Build** strategic public and private sector relationships,
- **Support** preparation, response, and remediation efforts relating to cybersecurity risks and incidents
- **Facilitate** cyber threat information sharing to improve understanding of cybersecurity risks and situational awareness
- **Raise** awareness of the financial, technical, and operational cybersecurity resources available to SLTT governments

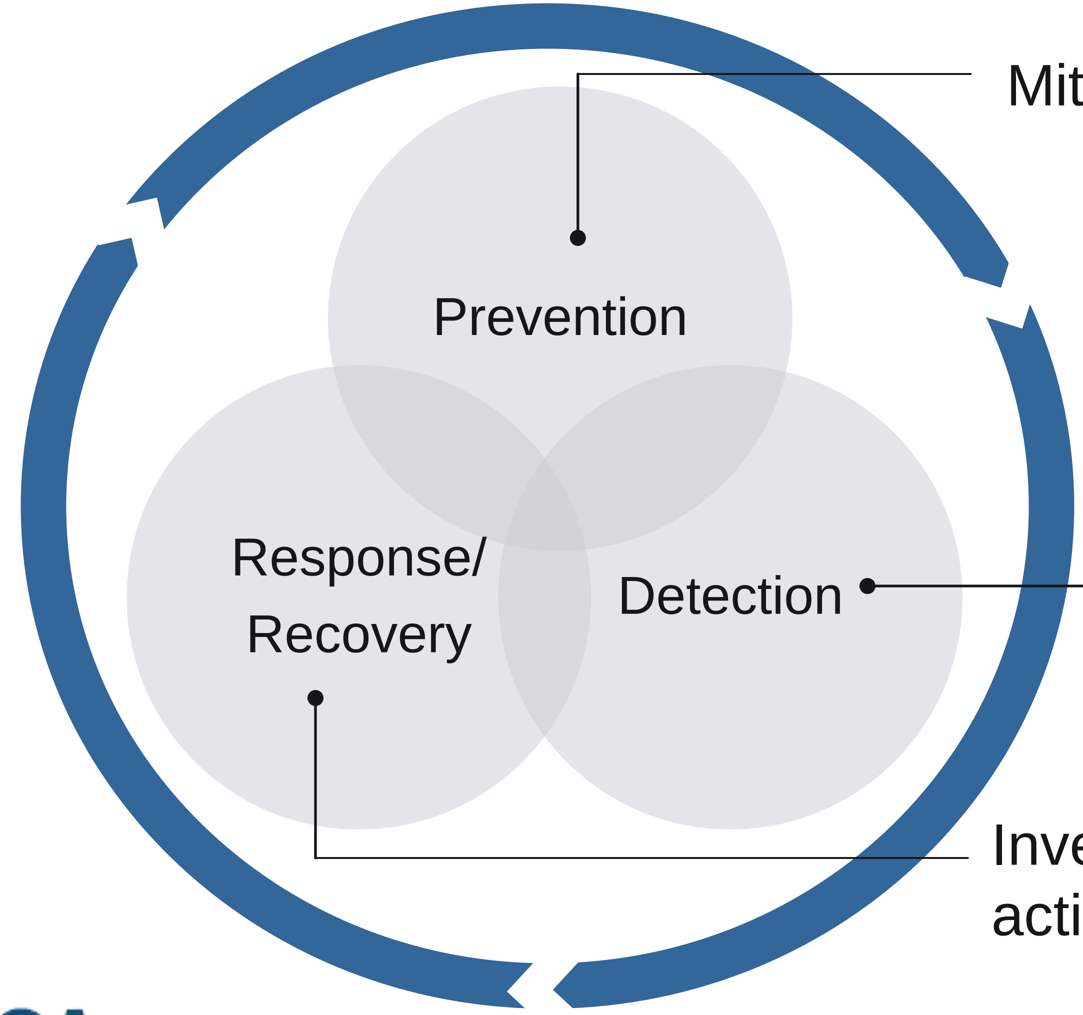
- **Support** cybersecurity training and exercises
- **Assist** in developing and coordinating vulnerability disclosure programs consistent with Federal and information security industry standards
- **Assist** SLTT governments in developing and coordinating cybersecurity plans
- **Coordinate** and perform other duties as necessary to achieve the goal of managing cybersecurity risks in the United States

UNDERSTANDING & MANAGING Risk

UNDERSTANDING RISK

- Identify inherent fraud risks
- Assess the likelihood and impact
- Determine tolerance
- Examine existing controls
- Prioritize residual risks
- Create a risk profile

MANAGING RISK



Mitigate the risk of fraud occurring

Discover potential fraud

Investigate, take corrective action, and reduce impacts

CURRENT DATA BREACH LANDSCAPE

Data Breach Specifics

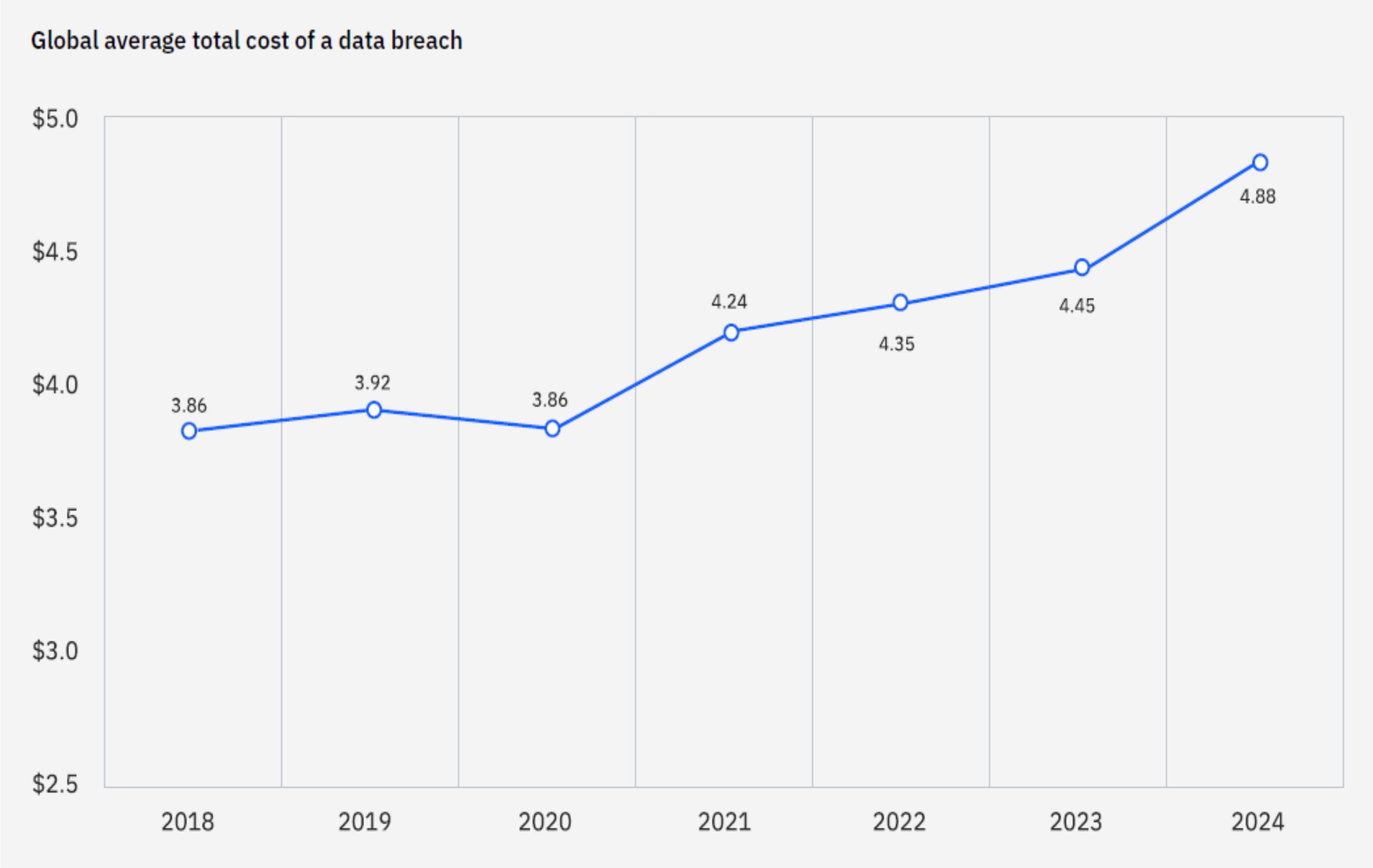
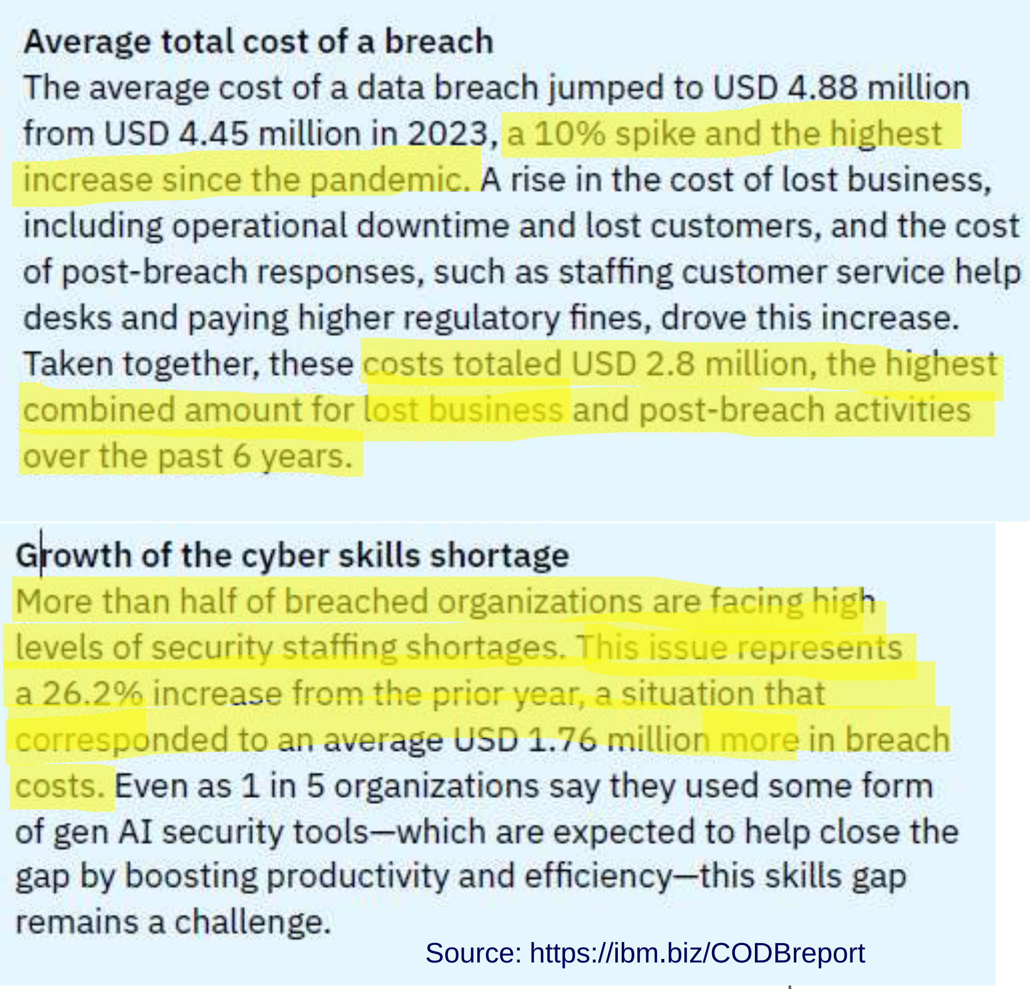

Global average total cost of a data breach

Figure 1. Measured in USD millions


Average total cost of a breach

The average cost of a data breach jumped to USD 4.88 million from USD 4.45 million in 2023, a 10% spike and the highest increase since the pandemic. A rise in the cost of lost business, including operational downtime and lost customers, and the cost of post-breach responses, such as staffing customer service help desks and paying higher regulatory fines, drove this increase. Taken together, these costs totaled USD 2.8 million, the highest combined amount for lost business and post-breach activities over the past 6 years.

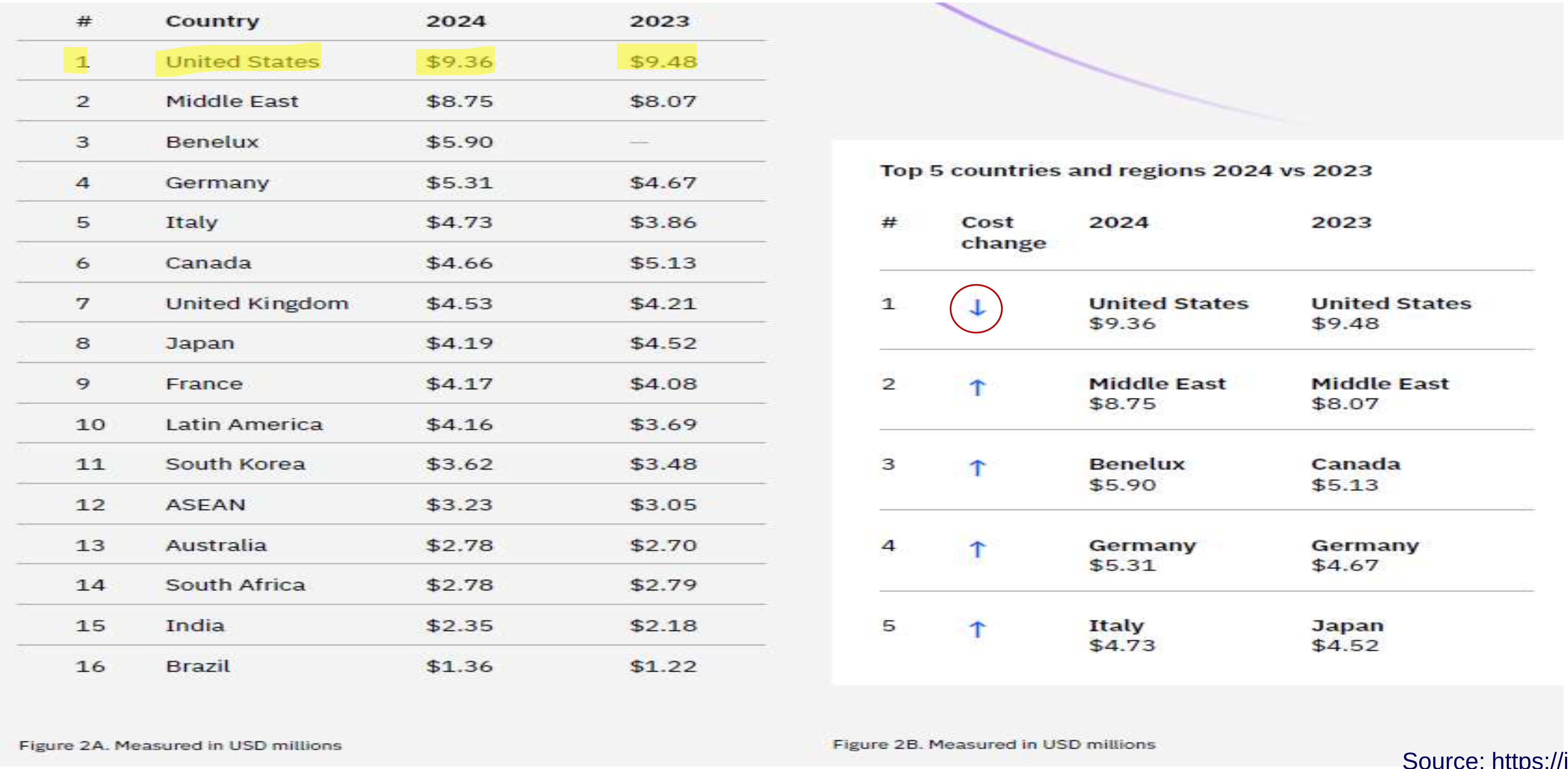
Growth of the cyber skills shortage

More than half of breached organizations are facing high levels of security staffing shortages. This issue represents a 26.2% increase from the prior year, a situation that corresponded to an average USD 1.76 million more in breach costs. Even as 1 in 5 organizations say they used some form of gen AI security tools—which are expected to help close the gap by boosting productivity and efficiency—this skills gap remains a challenge.

Source: https://ibm.biz/CODBreport

Data Breach Specifics

Data Breach Cost by Country / Region



#	Country	2024	2023
1	United States	$9.36	$9.48
2	Middle East	$8.75	$8.07
3	Benelux	$5.90	—
4	Germany	$5.31	$4.67
5	Italy	$4.73	$3.86
6	Canada	$4.66	$5.13
7	United Kingdom	$4.53	$4.21
8	Japan	$4.19	$4.52
9	France	$4.17	$4.08
10	Latin America	$4.16	$3.69
11	South Korea	$3.62	$3.48
12	ASEAN	$3.23	$3.05
13	Australia	$2.78	$2.70
14	South Africa	$2.78	$2.79
15	India	$2.35	$2.18
16	Brazil	$1.36	$1.22

Figure 2A. Measured in USD millions

Top 5 countries and regions 2024 vs 2023

#	Cost change	2024	2023
1	↓	United States $9.36	United States $9.48
2	↑	Middle East $8.75	Middle East $8.07
3	↑	Benelux $5.90	Canada $5.13
4	↑	Germany $5.31	Germany $4.67
5	↑	Italy $4.73	Japan $4.52

Figure 2B. Measured in USD millions

Source: https://ibm.biz/CODBreport

Data Breach Specifics

Cost of Data Breaches By Industry

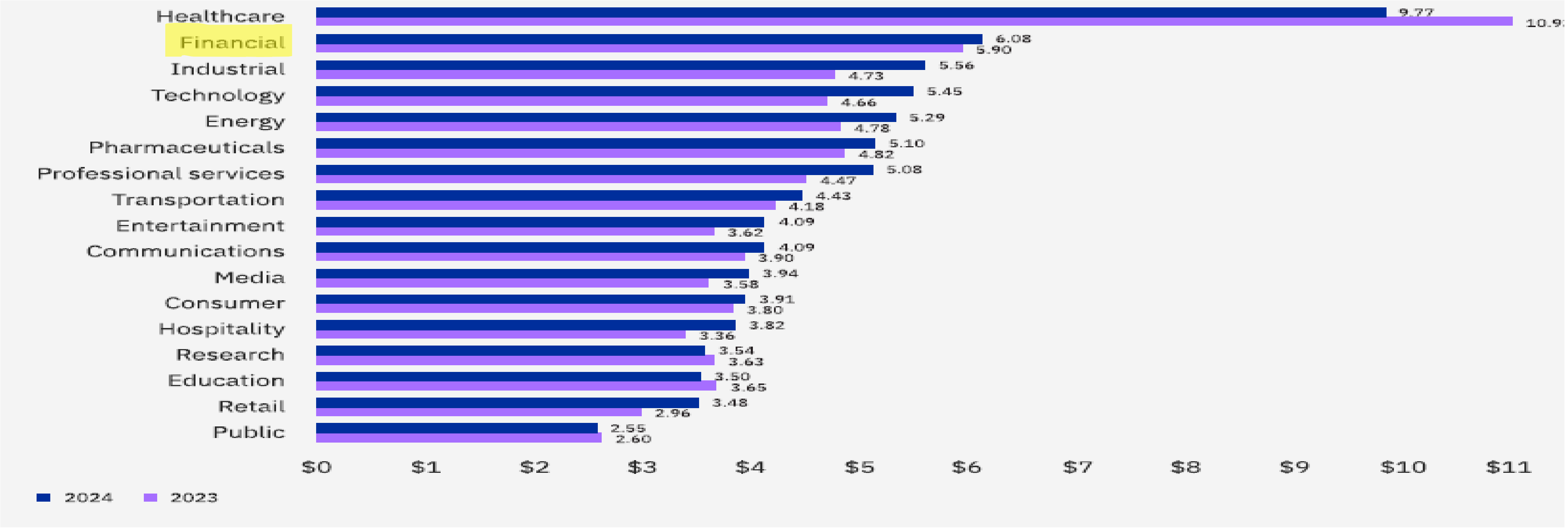


Figure 3. Measured in USD millions

Source: https://ibm.biz/CODBreport

Data Breach Specifics

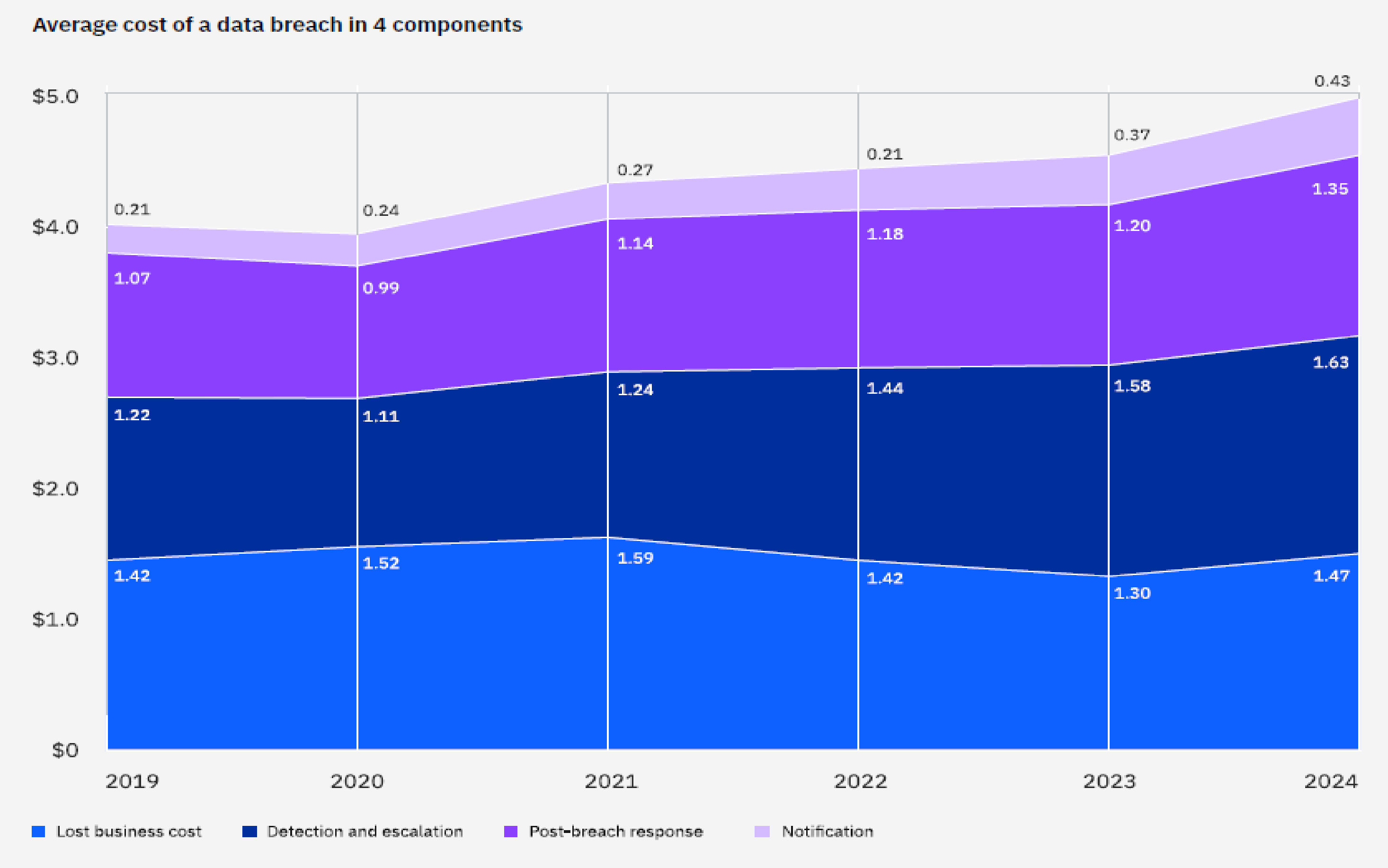


Figure 5. Measured in USD millions

Lost Business Cost and Post-Breach Response Costs Soared

- Costs from lost business and post-breach response rose nearly 11 percent over the previous year, which contributed to the significant rise in overall breach costs.
- Lost business costs include revenue loss due to system downtime, and the cost of lost customers and reputation damage.
- Post-breach costs can include the expense of setting up call centers and credit monitoring services for impacted customers and paying regulatory fines.

Source: https://ibm.biz/CODBreport

Data Breach Specifics

Time to Identify and Contain a Data Breach

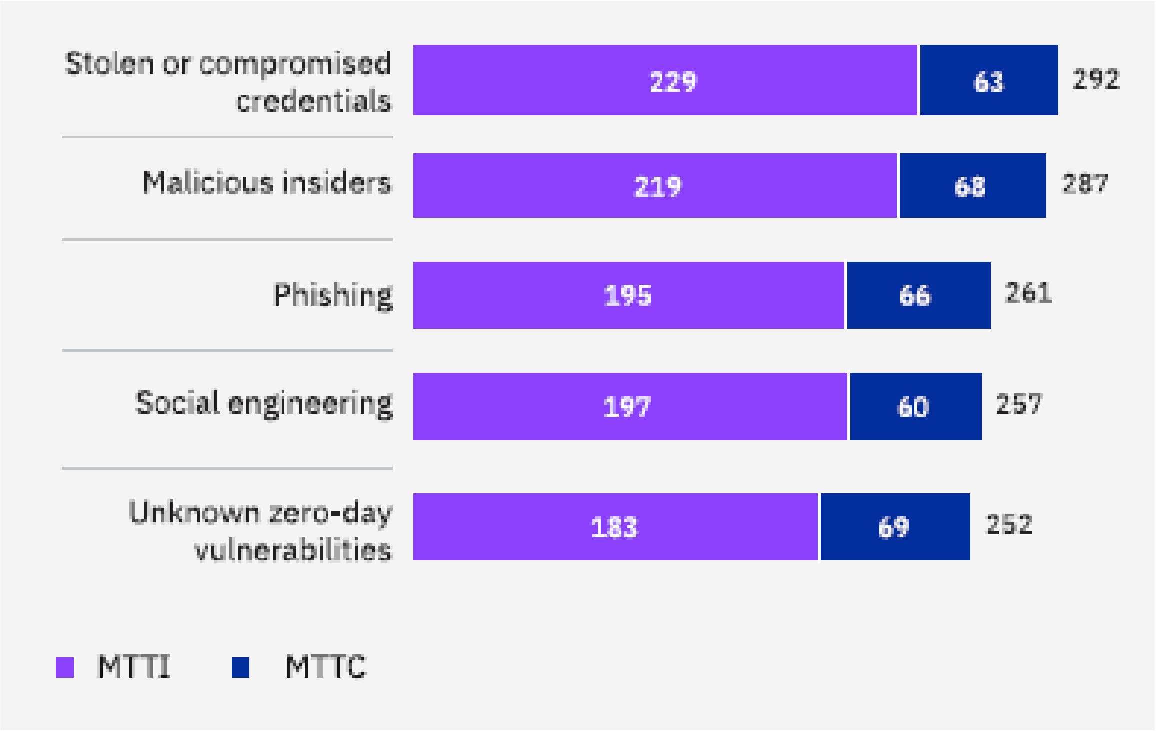


Figure 8. Measured in days

- Credential-based attacks Took Longer to Identity and Contain.
- Threat Identification Times Increased - Defenders Needed Time to Distinguish Between Legitimate and Malicious User Activity on Network.
- Zero-Day Vulnerabilities Most Time-Consuming to Contain

MTTI = Mean Time To Identity
MTTC – Mean Time to Contain

Source: https://ibm.biz/CODBreport

Data Breach Specifics

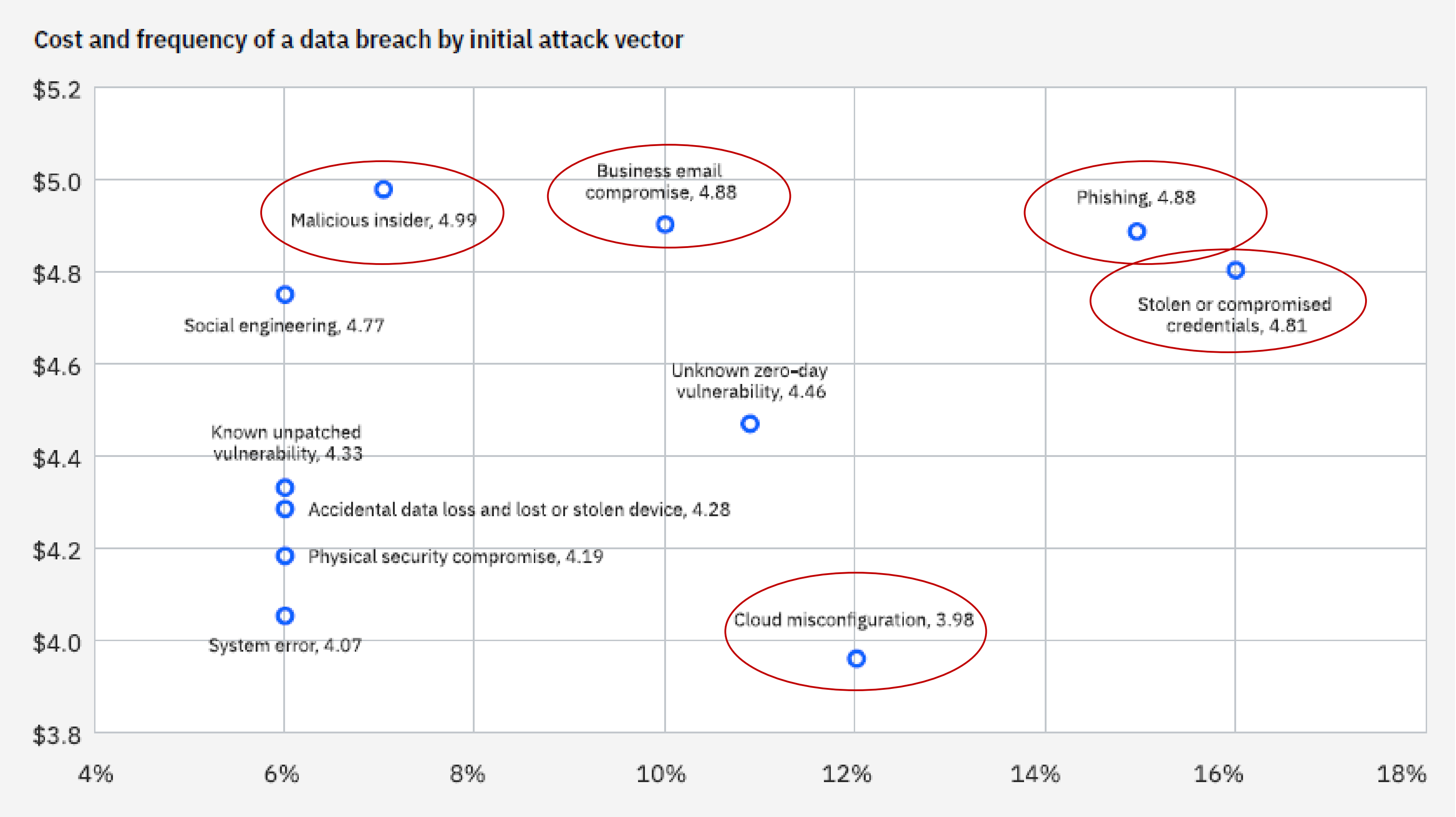


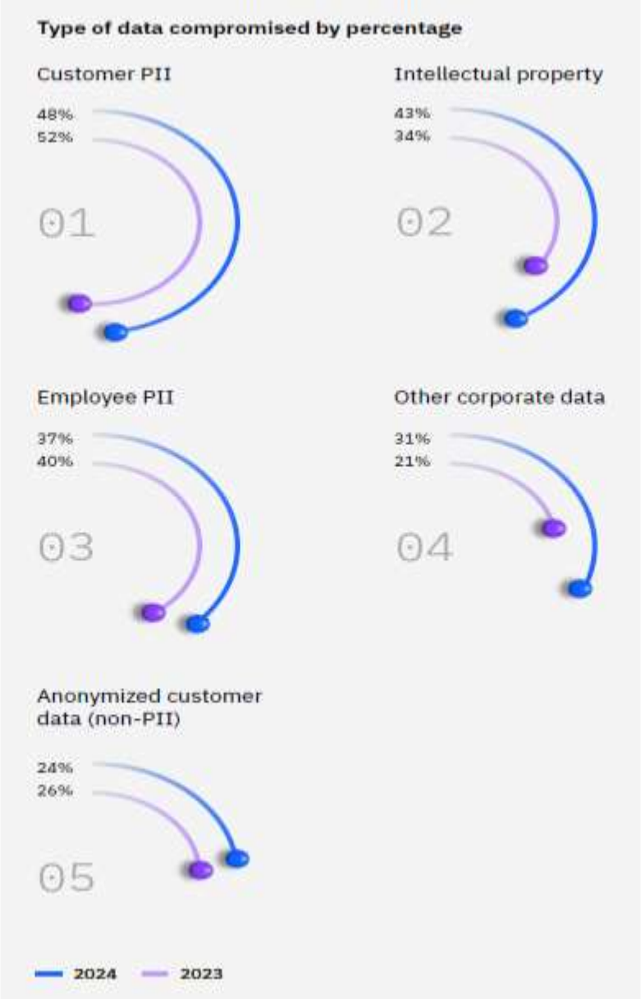
Figure 7. Measured in USD millions; percentage of all breaches

Initial Attack Vectors & Root Causes

- Phishing & Stolen or Compromised Credentials
  - Ranked Top 2 Most Prevalent Attack Vectors 2nd Year In A Row
  - Ranked Among Top 4 Costliest Incident Types
- Compromised Credentials
  - Benefited Attackers in 16 Percent of Breaches
  - Accounted for $4.81M (average)/Breach
- Phishing
  - Came in Close Second – Benefited Attackers in 15 Percent of Breaches
  - Accounted for $4.88M (average)/Breach

Source: https://ibm.biz/CODBreport

Data Breach Specifics



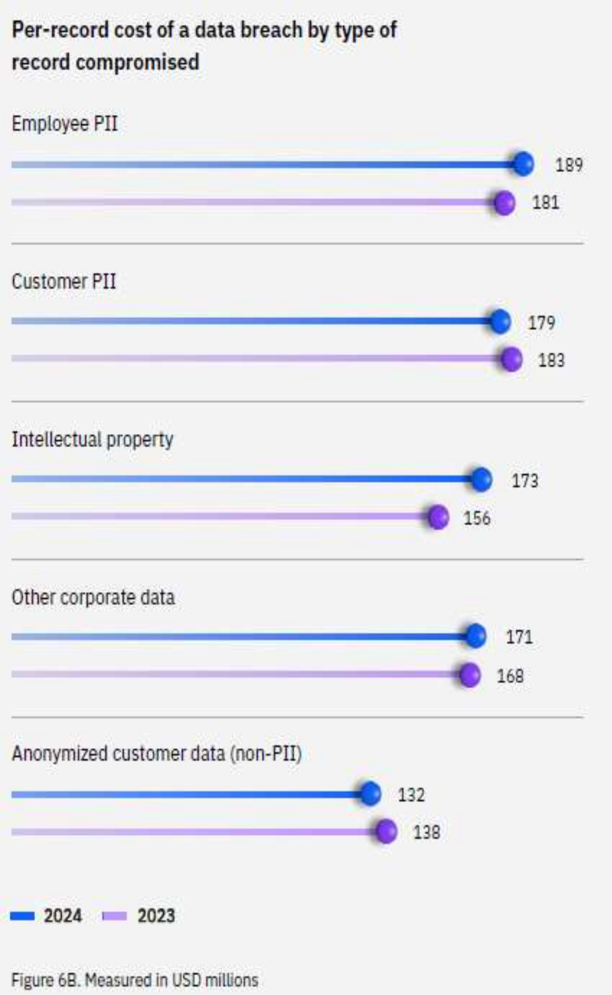


Figure 6B. Measured in USD millions

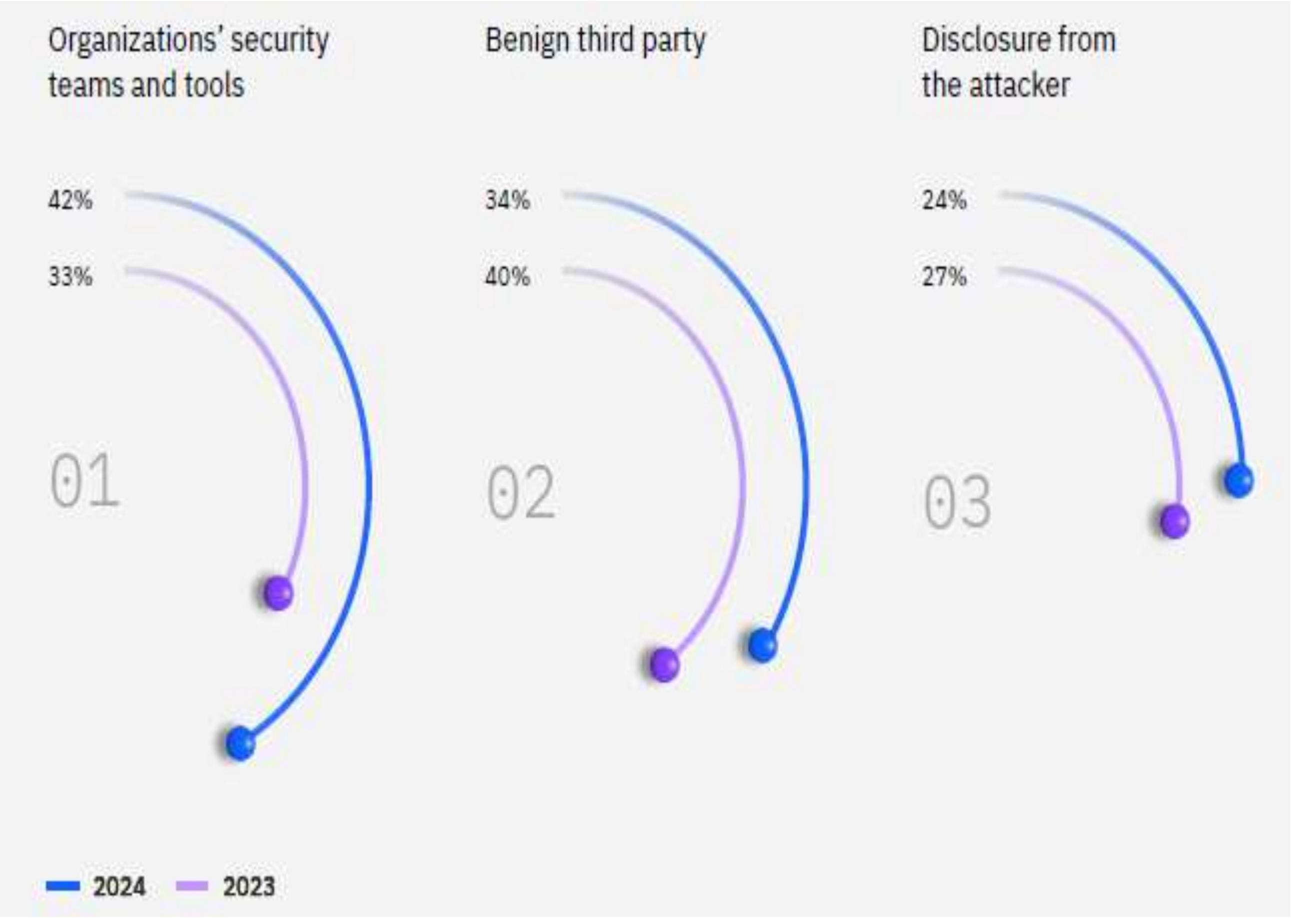
PII Compromises By the Numbers

- **Most Common Type of Data Stolen or Compromised**
  - Customer PII (48 Percent)
    - Tax ID Numbers
    - Emails
    - Home Addresses
  - Typically used in Identity Theft and Credit Card Fraud

- **Costliest Type of Data Stolen / Compromised**
  - Employee PII ($189M USD)

Source: https://ibm.biz/CODBreport

Data Breach Specifics



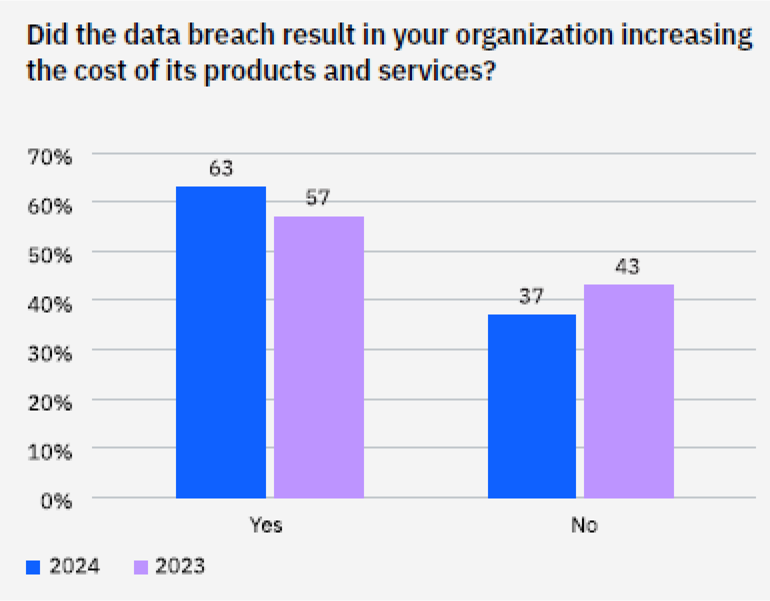
Who Identifies the Breach and How Quickly Makes a Difference in Resulting Data Breach Costs

- For 2024, Security Teams Working With Own Tools Improved Their Performance
- Other Cases Show Benign 3rd Parties Identified Data Breaches
  - Security Researchers, Law Enforcement, Consultants, CISA, ISACs/ISAOs
- Security Teams & Their Tools Detected Breaches Far More Often (42 Percent) than Benign 3rd Parties (34 Percent)
- Breaches Disclosed by Attacker Cost More ($5.53M Average) Due To Likely Have Achieved Objectives (i.e., Damage is Done)

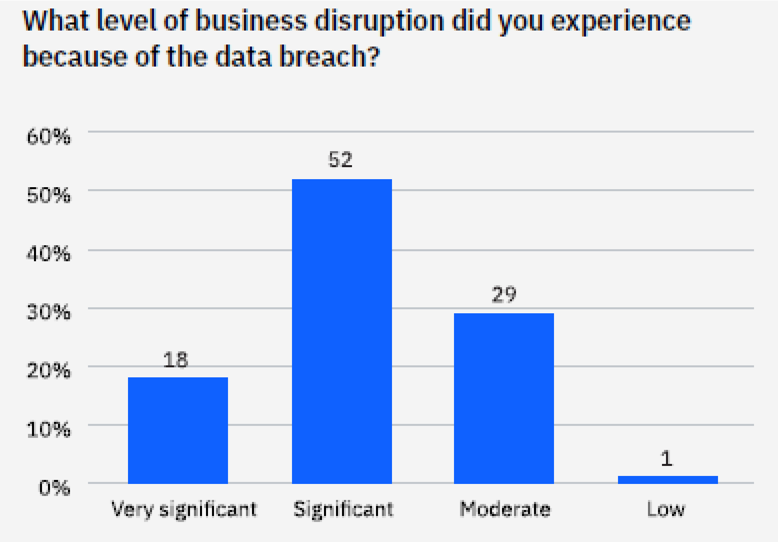
Best Approach: Leverage Both Security Team and Benign 3rd Party Resources

Source: https://ibm.biz/CODBreport

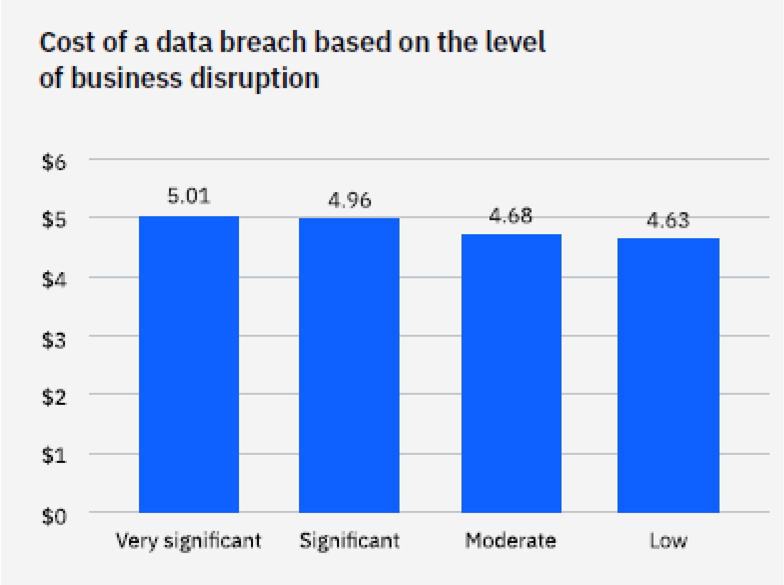
Data Breach Specifics



Did the data breach result in your organization increasing the cost of its products and services?



What level of business disruption did you experience because of the data breach?

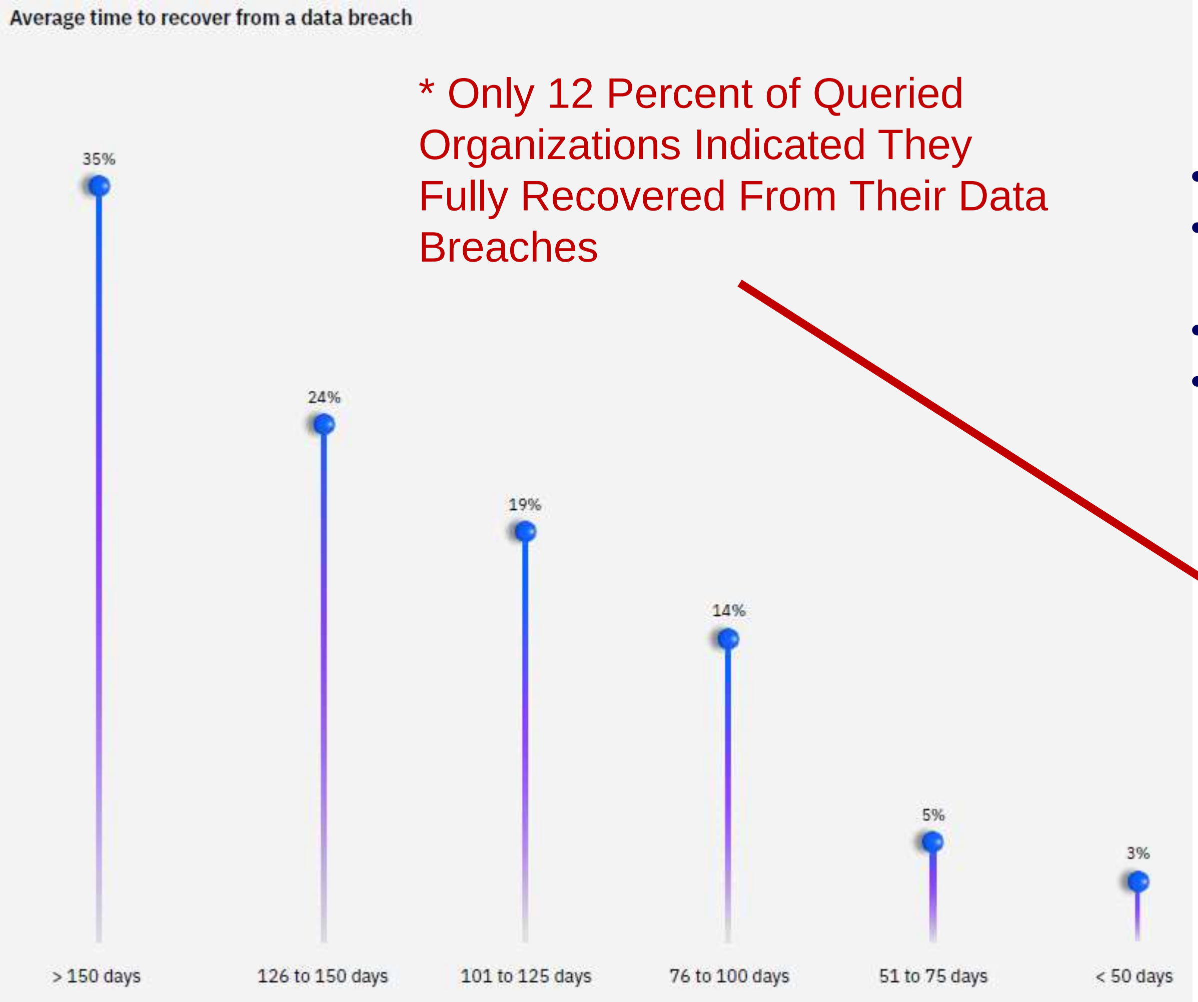


Cost of a data breach based on the level of business disruption

Figure 22. Measured in USD millions

Source: https://ibm.biz/CODBreport

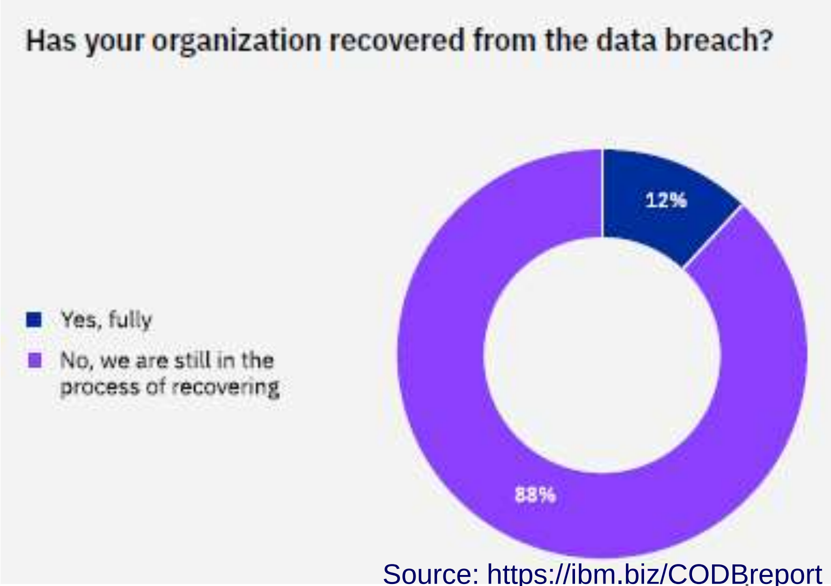
Data Breach Specifics



* Only 12 Percent of Queried Organizations Indicated They Fully Recovered From Their Data Breaches

Recovery Time Factors

- Business Areas Back to Normal In Areas Affected by Breach
- Organizations Have Met Compliance Obligations (Paying Fines)
- Customer Confidence and Employee Trust Restored
- Controls/Technologies/Expertise Put Into Place to Avoid Future Data Breaches

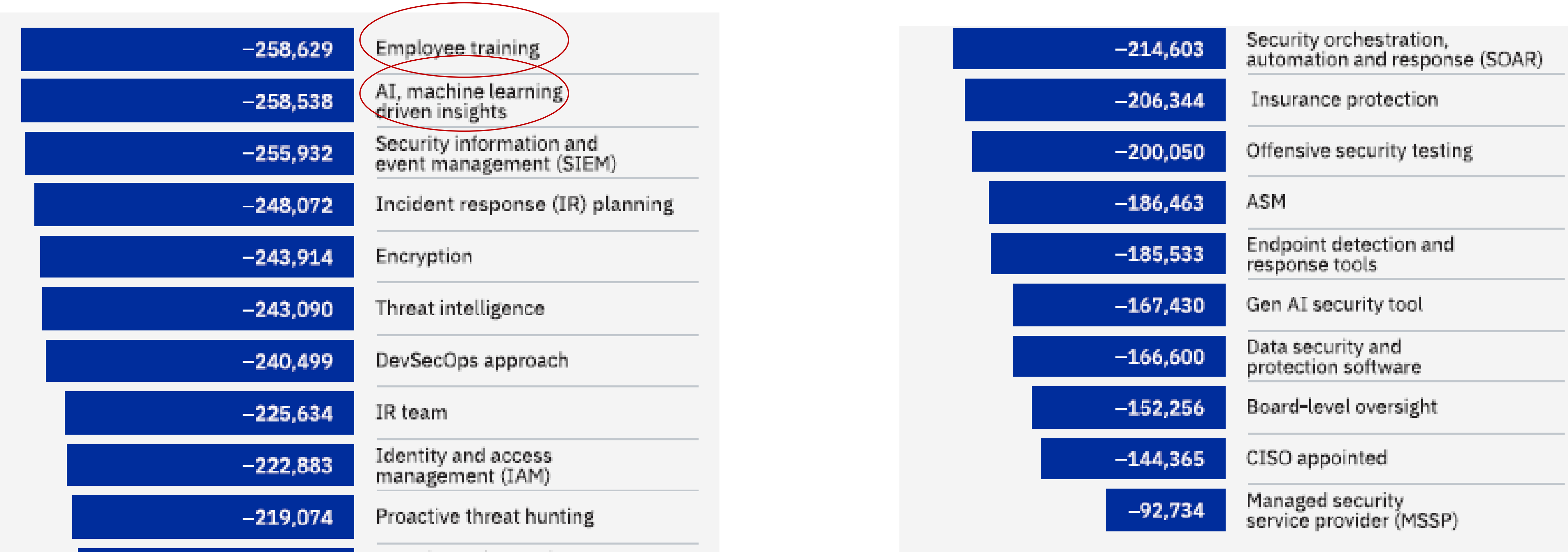


Source: https://ibm.biz/CODBreport

Data Breach Specifics

Factors That Reduced Average Breach Cost

(Cost Difference from $4.88M Breach Average)

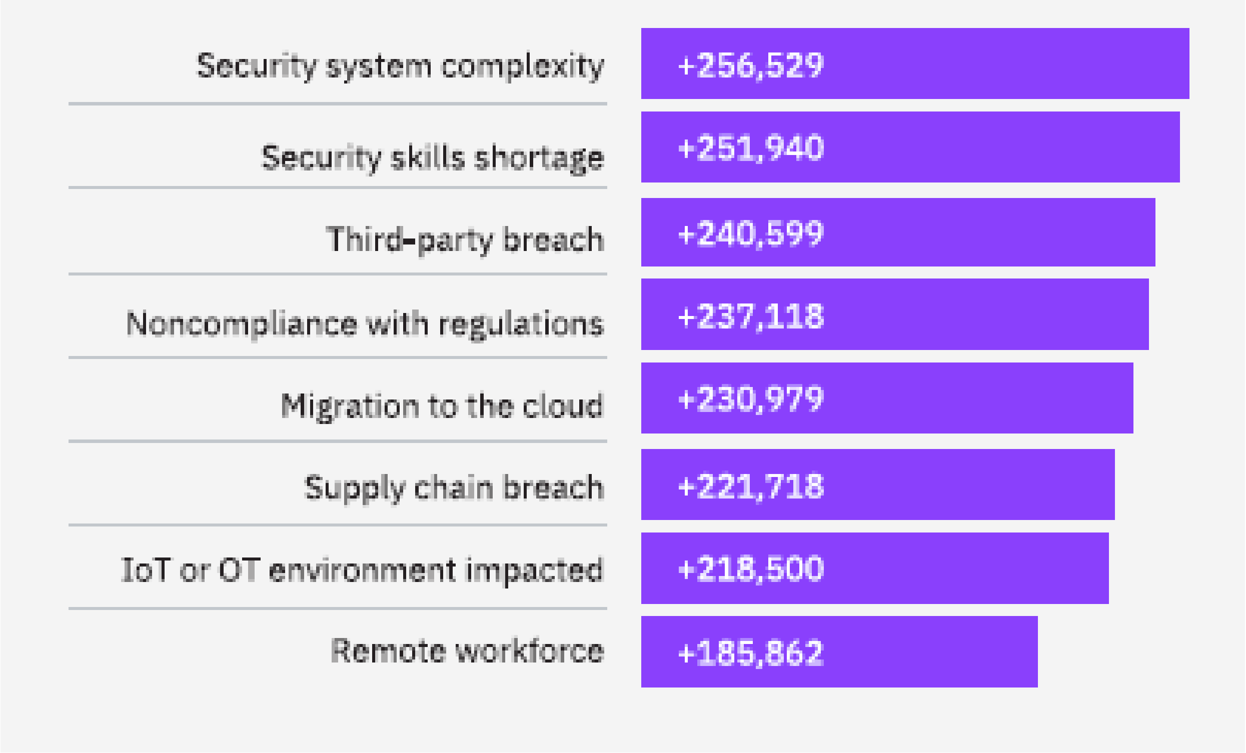


Source: https://ibm.biz/CODBreport

Data Breach Specifics

Factors That Increased Average Breach Cost

(Cost Difference from $4.88M Breach Average)



Source: https://ibm.biz/CODBreport

WHAT CAN YOU DO?

HOW CAN CISA HELP?

PROTECTIVE SECURITY ADVISOR (PSA) PROGRAM

Protective Security Advisor

Field-deployed personnel who serve as critical infrastructure security specialists

PSAs work with state, local, tribal, territorial (SLTT) and private sector as a link to CISA infrastructure protection resources such as:

- Security advice
- Information sharing
- Assessments
- Training
- Exercises

Secure at First Entry Assessment (PSA)

Rapid, high-level assessment of security posture and identification of options to mitigate relevant threats.

- Assess plans, information sharing, physical security, and security systems
- Written report with vulnerabilities and potential mitigation activities

Infrastructure Survey Tool (PSA)

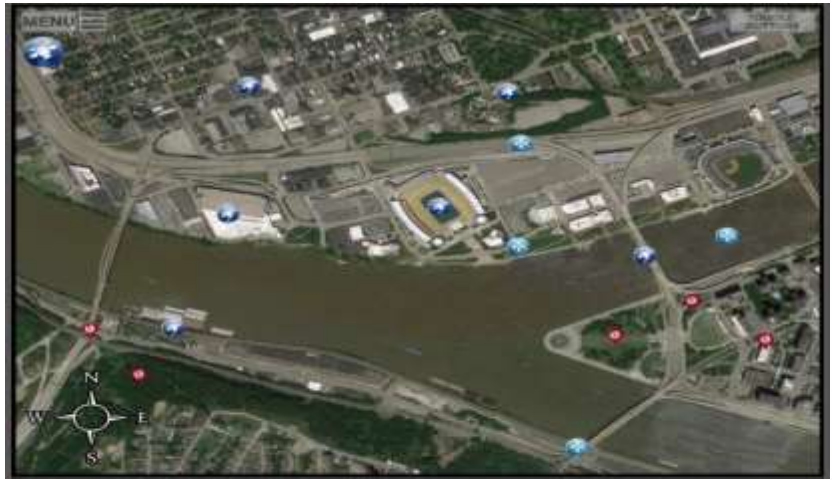
Comprehensive, in-depth vulnerability survey that applies weighted scores to identify vulnerabilities and trends across sectors.

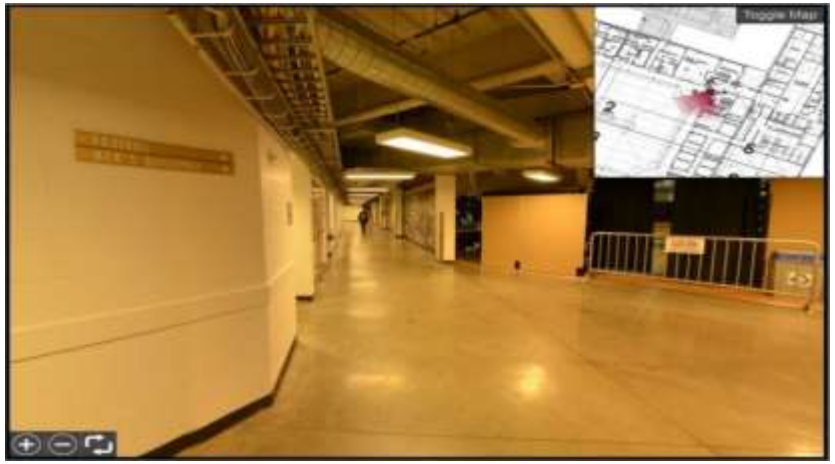
- Assess physical security, security force, security and resilience management, information sharing, and dependencies
- Identify areas of possible improvement
- Create measure indices that show comparisons
- Track progress

Infrastructure Visualization Platform (PSA)

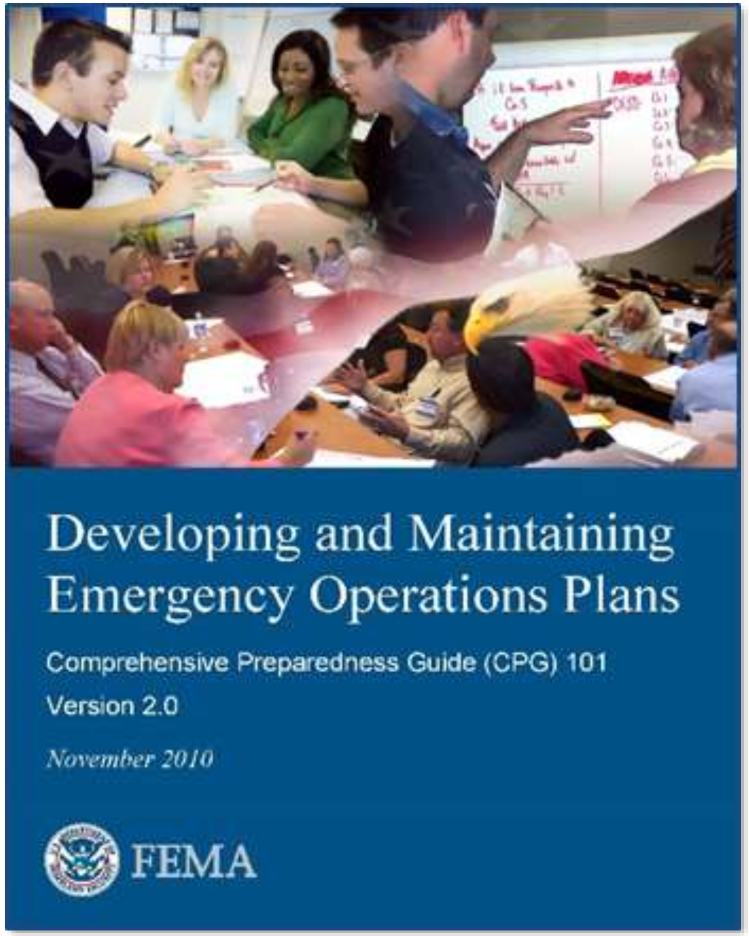
Combines immersive imagery, geospatial information and hypermedia data.

- Supports critical infrastructure security, special event planning, and response operations
- High-resolution, interactive visual data





Planning (PSA)



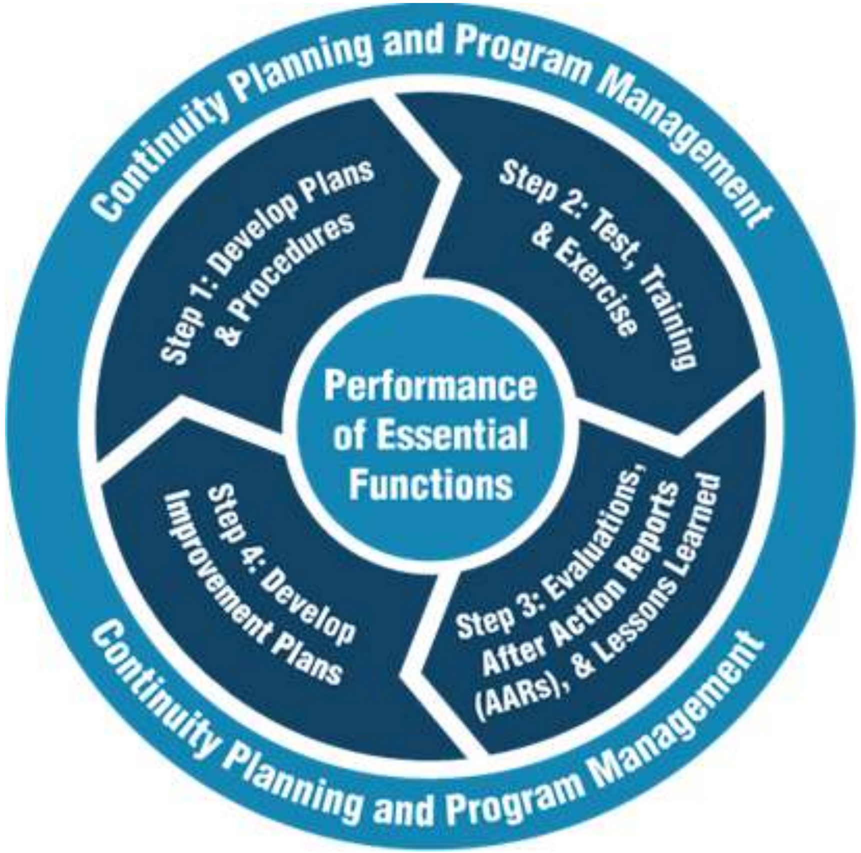
Developing and Maintaining Emergency Operations Plans

Comprehensive Preparedness Guide (CPG) 101

Version 2.0

November 2010

FEMA



Continuity Planning and Program Management
Step 1: Develop Plans & Procedures
Step 2: Test, Training & Exercise
Step 3: Evaluations, After Action Reports (AARs), & Lessons Learned
Step 4: Develop Improvement Plans
Performance of Essential Functions
Continuity Planning and Program Management

Training (PSA)

Protective Security Training

- Active Assailant Preparedness
- De-escalation & Non-confrontational Techniques
- The Power of Hello
- Insider Threat Mitigation
- Situational Awareness
- Supply Chain Integrity
- Suspicious Activity
- Information & Intelligence Sharing

Office for Bombing Prevention Training

- Bombing Prevention Awareness Program
- Bomb Threat Management Planning
- IED Awareness and Safety
- Bomb Threat Assessment for Decision Makers

Exercise (PSA)

Exercise Planning and Conduct

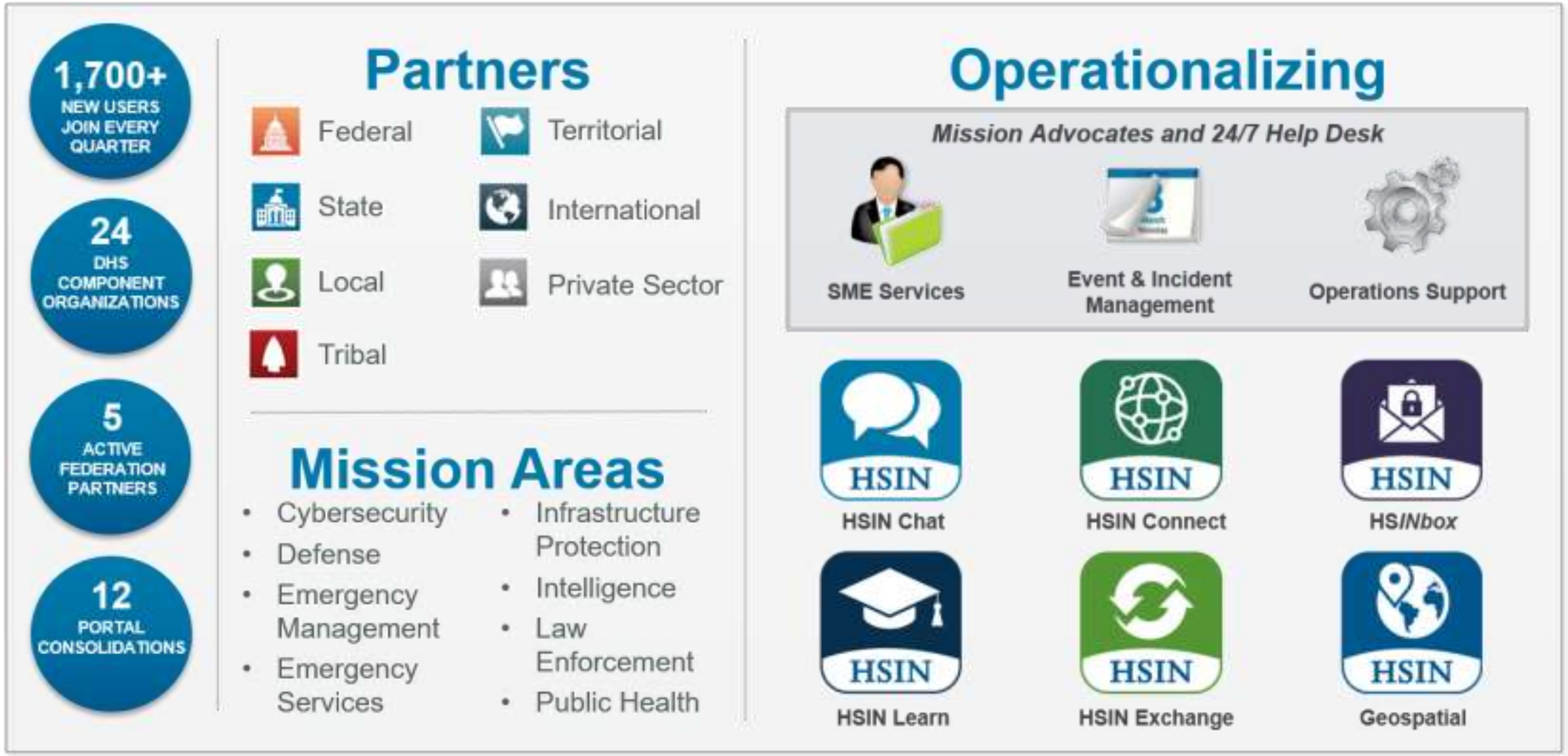
- Virtual or In-person
- Small to large scale
- Drill
- Tabletop/Discussion-based
- Functional/Operations-based

CISA Tabletop Exercise Package

- Discussion-based
- Pre-built templates
  - Objectives, scenario, discussion questions, resources
- 100+ scenarios

Information Exchange

Homeland Security Information Network (HSIN)



1,700+ NEW USERS JOIN EVERY QUARTER

24 DHS COMPONENT ORGANIZATIONS

5 ACTIVE FEDERATION PARTNERS

12 PORTAL CONSOLIDATIONS

Partners

Federal	Territorial
State	International
Local	Private Sector
Tribal	

Mission Areas

- Cybersecurity
- Defense
- Emergency Management
- Emergency Services
- Infrastructure Protection
- Intelligence
- Law Enforcement
- Public Health

Operationalizing

Mission Advocates and 24/7 Help Desk

SME Services

Event & Incident Management

Operations Support

What Can You Do – How CISA Can Help

- Harden Network Environment
  - **Know Your Network**
    - *Take Inventory - Maintain Updated Hardware/Software Lists,* Replace all EOL network equipment
    - *Know What Devices Should (NOT) Be On Network*
  - ***Employ Network Segmentation, Perimeter Security (DMZ, F/W, IDS/IPS), Endpoint Security***
  - ***Harden All Network Devices/Hosts/Clients***
    - ***- Payment Card Industry Data Security Standard (PCI DSS), CIS Benchmarks, STIGs, etc.***
  - ***Encrypt Data At Rest and In Transit (VPNs)***
    - *Don't Forget To Encrypt Backups Too!*
  - ***Employ Strong Zero-Trust/Least Privilege Identity and Access Management (IAM) Policies***
    - *Use Strong, Complex, Unique Passwords - Implement MFA For* ***ALL*** *Access (General & Administrative)*
    - *On-Premise / Remote / Cloud Environments*
  - ***Patch – Patch – Patch!!***
    - Keep Network Devices And All System Software Updated With Latest Available Versions
  - ***Establish Allow Lists***
    - Whitelist for only authorized IP addresses – Refine to specific times of day and accounts

What Can You Do

- Harden Network Environment (Cont)
  - ***Employ Robust Log Policy* & Periodically Review for Anomalies**
    - Failed Attempts / Unusual Times / High Data Transfer Rates / Elevated Privileges
  - **Practice & Maintain Incident Response Plan (IRP) / Continuity of Operations Plan (COOP)**
  - ***Create Backups* – Multiple Encrypted Backups (System State, Files, Data, etc.)**
    - Familiarize Team with Factory Resets and Restoration Procedures
  - ***Safeguard / Update Network Topology Diagrams***
    - Always Apply Least Privilege and NTK to Network Diagrams – ONLY Trusted Personnel!!
    - Maintain Awareness of Internal/External Network Architecture Solicitation Efforts
  - ***Be Aware of Cyber/Physical-Enabled Threats***
    - Adversaries May Attempt to Obtain Network Creds by Office Visits, Tradeshow/Conference Conversations, Social Media Platforms

What Can You Do

- Limit Adversarial Use of Common Vulnerabilities

Informational Activities

- Shields Up / Shields Ready!!
- Cyber Threat Indicator/ Defensive Measure Information Sharing Services

Preparedness Activities

- Known Exploitable Vulnerabilities (KEV) Catalog
- Cyber Hygiene Vulnerability / Web App Scanning
- Strategic Resiliency Evaluations/Assessments
- Technical Assessments (Penetration Testing, Risk & Vulnerability Assessments, Validated Architecture Design Reviews)
- Cyber Exercises and “Playbooks”
- *** Cyber Security Evaluation Tool (CSET) ***
  - CISA GitHub: Downloading and Installing CSET | CISA

Response Assistance

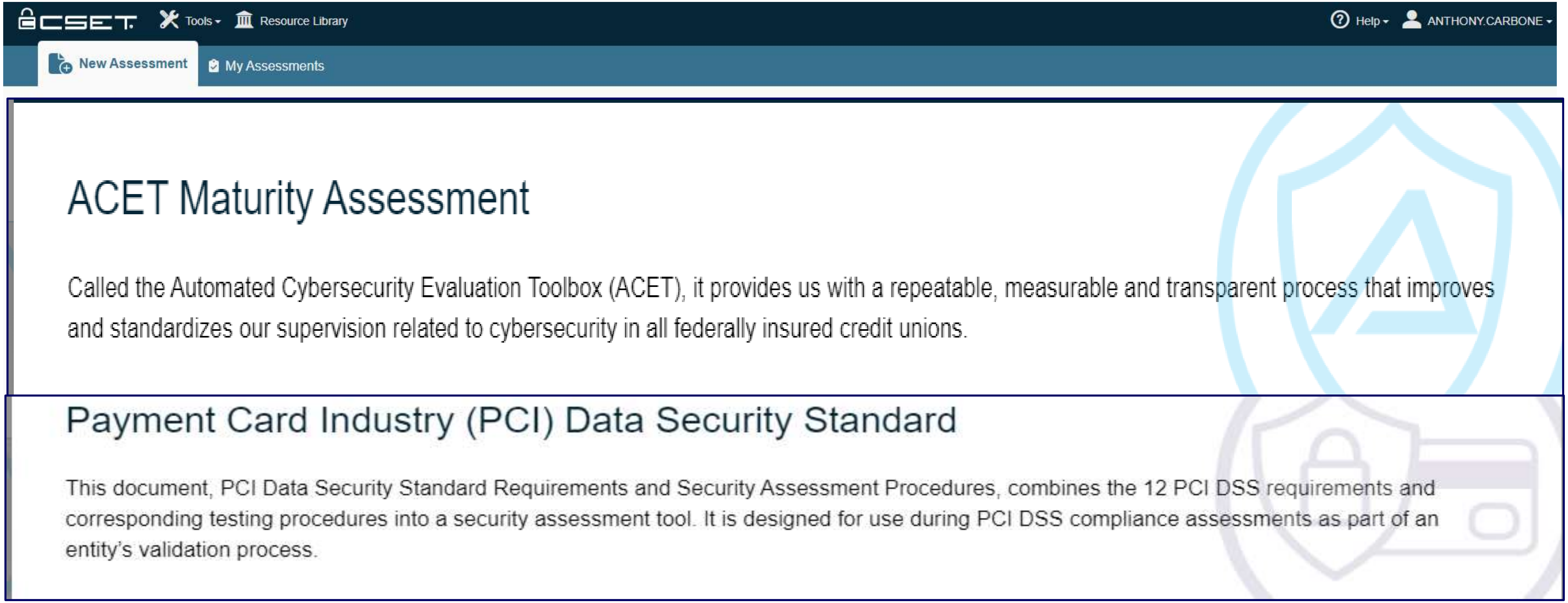
- Remote / On-Site Assistance
- Vulnerability Entity Notification
- APT/Pre-Ransomware Notification Initiative
- Malware Analysis
- Hunt and Incident Response Teams
- Incident assistance coordination

Full CISA Service Catalog:

CISA Services Catalog | CISA

NO-COST SERVICES Available To All SLTT and Critical Infrastructure Partners

What Can You Do



ACET Maturity Assessment

Called the Automated Cybersecurity Evaluation Toolbox (ACET), it provides us with a repeatable, measurable and transparent process that improves and standardizes our supervision related to cybersecurity in all federally insured credit unions.

Payment Card Industry (PCI) Data Security Standard

This document, PCI Data Security Standard Requirements and Security Assessment Procedures, combines the 12 PCI DSS requirements and corresponding testing procedures into a security assessment tool. It is designed for use during PCI DSS compliance assessments as part of an entity's validation process.

What Can You Do

- Train & Exercise
  - Have Tailored Up-To-Date Contingency Plans On Hand and Exercise Frequently

Incident Management Planning Helps Mitigate Effects

1. Get leadership support for incident management planning.
2. Establish an event-detection process.
3. Establish a triage-and-analysis process.
4. Establish an incident-declaration process.
5. Establish an incident-response and recovery process.
6. Establish an incident-communications process.
7. Assign roles and responsibilities for incident management.
8. Establish a post-incident analysis and improvement process.

Resources:

- *CRR Supplemental Resource Guide, Incident Management*
- *Cybersecurity Incident & Vulnerability Playbook*
- *NIST (800 Special Publication Series)*

CRR Supplemental Resource Guide

Volume 5

Incident Management

Version 1.1

TLP:WHITE

Cybersecurity Incident & Vulnerability Response Playbooks

Operational Procedures for Planning and Conducting Cybersecurity Incident and Vulnerability Response Activities in FCEB Information Systems

Publication: November 2021

Cybersecurity and Infrastructure Security Agency

DISCLAIMER: [illegible]

TLP:WHITE

CISA CYBER+INFRASTRUCTURE

What Can You Do

- Train & Exercise
  - Have a Tailored Incident Response Plan On Hand
  - Formal Cyber User Training / Workshops (Don’t Click on Unknown Links/Attachments)
    - Train Employees On Their Cybersecurity Roles
      - Good Cybersecurity Practices
        - Strong Passwords
        - Effective Password Management
        - Least Privilige
        - Not Visiting Unknown Websites
        - Not Clicking On Unfamiliar/Untrusted Links
      - Thwarting Phishing Attempts

NICCS

CISA offers easily accessible education and awareness resources through the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

The NICCS website includes:

- Searchable Training Catalog with 4,400 plus cyber-related courses offered by nationwide cybersecurity educators
- Interactive National Cybersecurity Workforce Framework
- Cybersecurity Program information: FedVTE, Scholarships for Service, Centers for Academic Excellence, and Cyber Competitions
- Tools and resources for cyber managers
- Upcoming cybersecurity events list

For more information, visit NICCS.CISA.gov

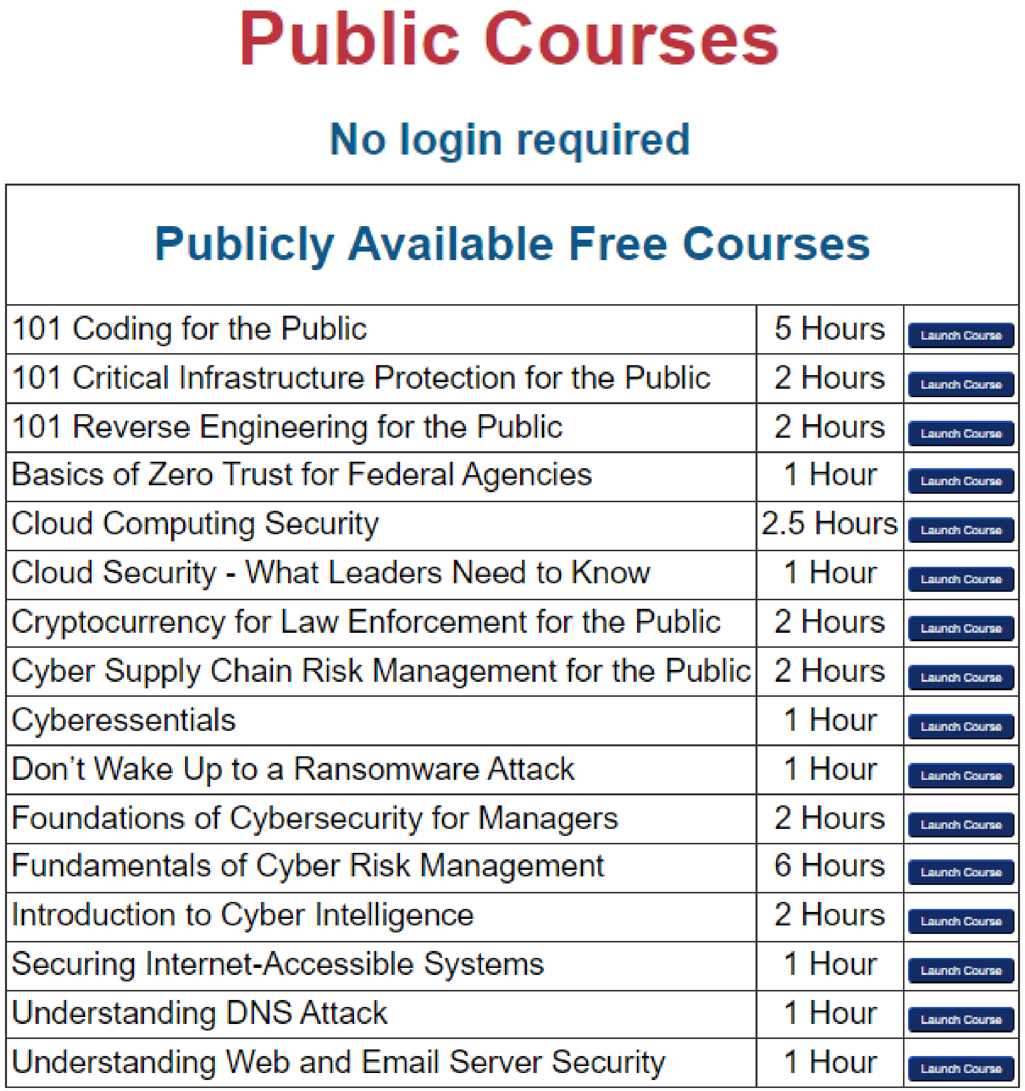
Free Federal Cyber Training

FedVTE FEDERAL VIRTUAL TRAINING ENVIRONMENT

FedVTE is an online, on-demand training center that provides **free** cybersecurity training for U.S. veterans and federal, state, local, tribal, and territorial government employees. **As of January 2017,** there are:

- Over 140,000 registered users, including employees at all levels of government
- Over 18,000 veteran users (through non-profit partner, Hire Our Heroes™)
- Over 5,000 SLTT registered users

https://fedvte.usalearning.gov/



Public Courses

No login required

Publicly Available Free Courses

101 Coding for the Public	5 Hours	Launch Course
101 Critical Infrastructure Protection for the Public	2 Hours	Launch Course
101 Reverse Engineering for the Public	2 Hours	Launch Course
Basics of Zero Trust for Federal Agencies	1 Hour	Launch Course
Cloud Computing Security	2.5 Hours	Launch Course
Cloud Security - What Leaders Need to Know	1 Hour	Launch Course
Cryptocurrency for Law Enforcement for the Public	2 Hours	Launch Course
Cyber Supply Chain Risk Management for the Public	2 Hours	Launch Course
Cyberessentials	1 Hour	Launch Course
Don't Wake Up to a Ransomware Attack	1 Hour	Launch Course
Foundations of Cybersecurity for Managers	2 Hours	Launch Course
Fundamentals of Cyber Risk Management	6 Hours	Launch Course
Introduction to Cyber Intelligence	2 Hours	Launch Course
Securing Internet-Accessible Systems	1 Hour	Launch Course
Understanding DNS Attack	1 Hour	Launch Course
Understanding Web and Email Server Security	1 Hour	Launch Course

Workshops

Goal / Takeaway

- Provide organization with tangible, useful information related to risk-based decision making / security planning
- **4-Hour collaborative session**
- **Tailored** to concerns/threats of specific sector
- **Opportunity for security professionals to learn together**

Subject Areas / Topics

- Cyber Resilience
- Critical Service Determination
- Cyber Incident Management
- External /3rd Party Dependencies
- Election Security
- **Topic of Your Choice**

Common Participants

- IT Policy/Governance (CISO)
- IT Security Planning/Management (Dir of IT)
- IT Infra (System/Network Administrators)
- IT Ops (Configuration/Change Managers)
- Business Ops/Continuity
- Risk Management
- Procurement/Vendor Management

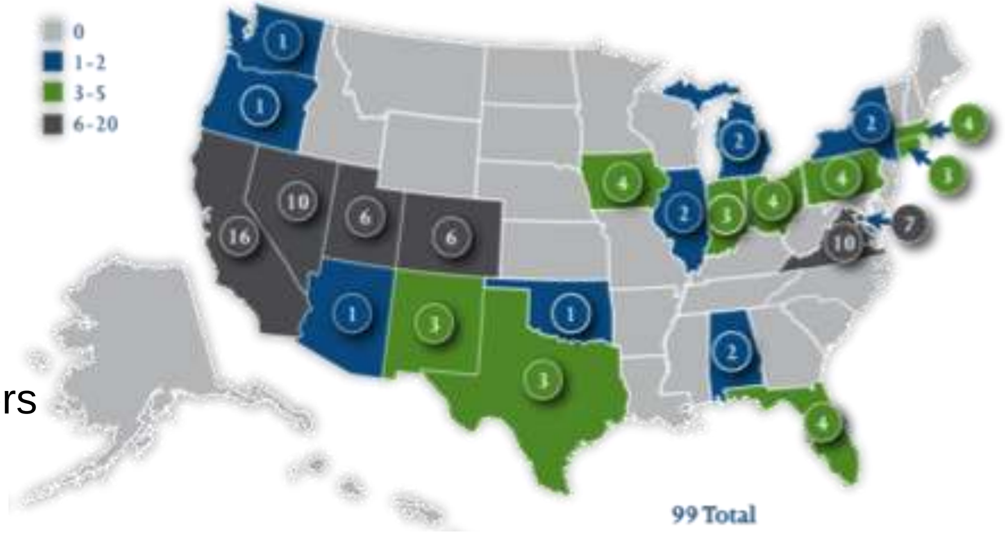
What Can You Do

- Train & Exercise
  - Have a Tailored Incident Response Plan On Hand
  - Formal Cyber User Training / Workshops (Don’t Click on Unknown Links/Attachments)
  - Exercise – Exercise – Exercise!!
    - Backup/Restoration Events, Practice Switching to Manual Ops, Table-Top Exercises (TTXs)

Cyber Exercises and Planning

CISA’s National Cyber Exercise and Planning Program develops, conducts, and evaluates cyber exercises and planning activities for state, local, tribal and territorial governments and public and private sector critical infrastructure organizations.

- Cyber Storm Exercise – DHS’s flagship national-level biennial exercise
- Exercise Planning and Conduct
- Cyber Exercise Consulting and Subject Expertise Support
- Cyber Planning Support
- Off-the-Shelf Resources



Also Offers CISA Tabletop Exercise Packages (CTEPs)

- Comprehensive set of resources designed to assist stakeholders in conducting their own exercises.
- CTEP Package found at: CISA Tabletop Exercise Packages | CISA

What Can You Do

- Train & Exercise
  - Have a Tailored Incident Response Plan On Hand
  - Formal Cyber User Training / Workshops (Don’t Click on Unknown Links/Attachments)
  - Exercise – Exercise – Exercise!!
    - Backup/Restoration Events, Practice Switching to Manual Ops, Table-Top Exercises (TTXs)
- Share Information
  - ISAC/ISAO Membership
  - Cyber Threat Indicators (CTIs) / Defensive Measures (DMs)
  - Indicators of Compromise (IOCs)
  - Tactics, Techniques, Procedures (TTPs)

Information Sharing & Analysis Centers

- **ISACs and ISAOs:**
  - **Information Sharing and Analysis Centers** (ISACs) or **Organizations** (ISAOs) are communities of interest sharing cybersecurity risk, threat information, and incident management to members. For more information on ISACs, visit www.nationalisacs.org. For more on ISAOs visit www.isao.org/about.
- **Multi-State Information Sharing and Analysis Center:**
  - Focal point for cyber threat prevention, protection, response and recovery for state, local, tribal, and territorial governments.
  - Operates 24 x7 cyber security operations center, providing real-time network monitoring, early cyber threat warnings and advisories, vulnerability identification and mitigation and incident response. For more information, visit www.cisecurity.org/ms-isac or email info@msisac.org

Surface Transportation, Public Transportation and Over the Road Bus Information Sharing and Analysis Centers

Elections Infrastructure ISAC

MS-ISAC Multi-State Information Sharing & Analysis Center

ONG-ISAC

National Defense ISAC

CISA CYBER+INFRASTRUCTURE

Maritime Transportation System Information Sharing and Analysis Center

RETAIL & HOSPITALITY ISAC

M-E ISAC MEDIA + ENTERTAINMENT INFORMATION SHARING & ANALYSIS CENTER

REN-ISAC

FS-ISAC

Real Estate ISAC Information Sharing and Analysis Center Serving the Commercial Facilities Sector

IT ISAC

WATER ISAC

DNG-ISAC

E-ISAC

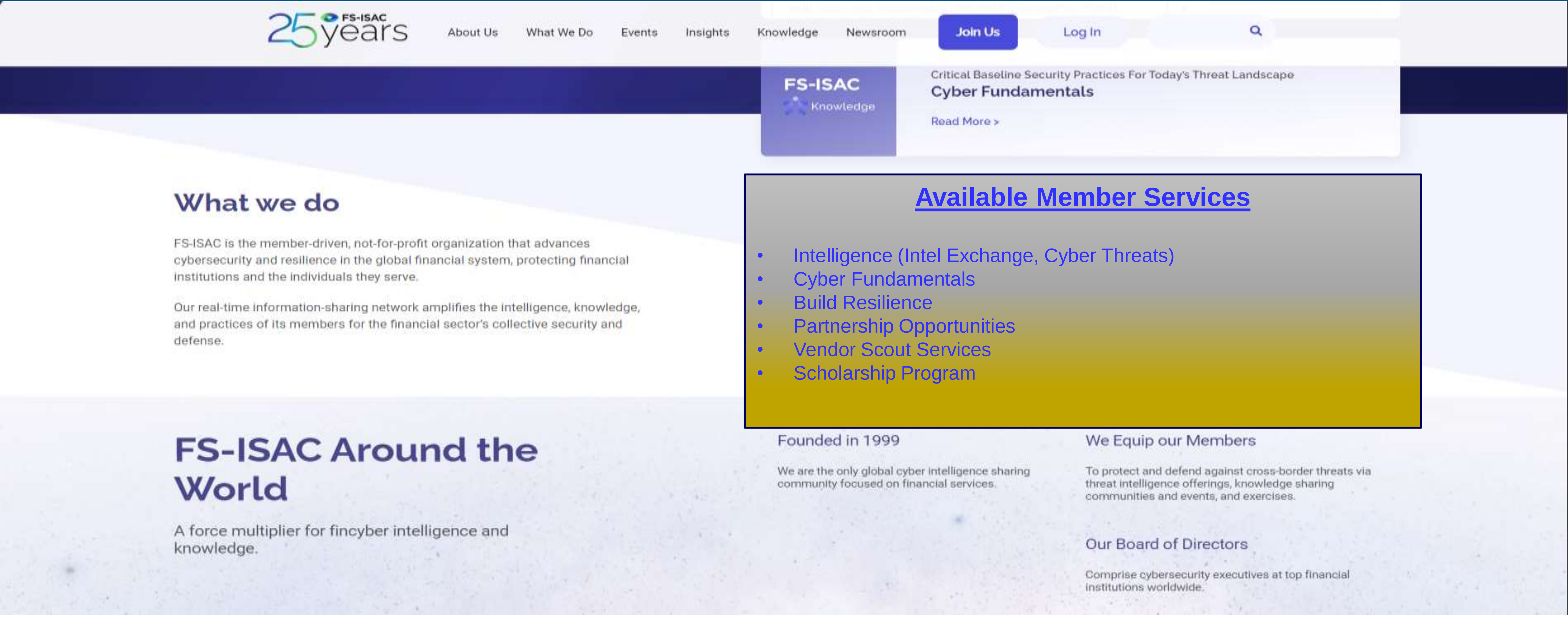
H-ISAC HEALTH - ISAC

AUTO-ISAC

SPACE ISAC

AVIATION ISAC

FS-ISAC



Critical Baseline Security Practices For Today's Threat Landscape

Cyber Fundamentals

What we do

FS-ISAC is the member-driven, not-for-profit organization that advances cybersecurity and resilience in the global financial system, protecting financial institutions and the individuals they serve.

Our real-time information-sharing network amplifies the intelligence, knowledge, and practices of its members for the financial sector's collective security and defense.

FS-ISAC Around the World

A force multiplier for fincyber intelligence and knowledge.

Founded in 1999

We are the only global cyber intelligence sharing community focused on financial services.

We Equip our Members

To protect and defend against cross-border threats via threat intelligence offerings, knowledge sharing communities and events, and exercises.

Our Board of Directors

Comprise cybersecurity executives at top financial institutions worldwide.

Available Member Services

- Intelligence (Intel Exchange, Cyber Threats)
- Cyber Fundamentals
- Build Resilience
- Partnership Opportunities
- Vendor Scout Services
- Scholarship Program

https://www.fsisac.com

CISA Region IV (South Carolina)

What Can You Do

- Train & Exercise
  - Have a Tailored Incident Response Plan On Hand
  - Formal Cyber User Training / Workshops (Don’t Click on Unknown Links/Attachments)
  - Exercise – Exercise – Exercise!!
    - Backup/Restoration Events, Practice Switching to Manual Ops, Table-Top Exercises (TTXs)
- Share Information
  - ISAC/ISAO Membership
  - Cyber Threat Indicators (CTIs) / Defensive Measures (DMs)
  - Indicators of Compromise (IOCs)
  - Tactics, Techniques, Procedures (TTPs)
- Report – Report – Report!!!

Incident Reporting

Why report cyber incidents?

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

When to report a cyber incident? (CIRCIA Is Coming!!)

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

Asset Response:

CISA Central - Provides Real-Time Threat Analysis and Incident Reporting Capabilities

24x7 Contact:

- Dial: 1-888-282-0870
- Email: Central@cisa.dhs.gov
- Web: www.cisa.gov/report

Threat Response:

1. South Carolina Law Enforcement Division (SLED) Critical Infrastructure Cybersecurity (SC CIC) Program

Contact:

- Dial: 803-896-8181
- Email: cyber@sled.sc.gov

2. Federal Bureau of Investigation (FBI)

Contact:

- Dial: 1-855-292-3937
- Email: cywatch@ic.fbi.gov
- Web: www.ic3.gov

3. Respective ISAC/ISAO Member

Questions / Next Step

General Inquiries

cisa.iod.region.r04_ops@cisa.dhs.gov

Columbia

PSA Keith Jones Email: keith.m.jones@hq.dhs.gov Cell: 803.218.8550	**CSC CL Clay** Email: cl.clay@cisa.dhs.gov Cell: 771.217.7652

Charleston / Mt. Pleasant

PSA Amanda Knight Email: amanda.knight@cisa.dhs.gov Cell: 771.217.1409	**CSA Anthony E. Carbone** Email: anthony.carbone@cisa.dhs.gov Cell: 771.215.7508