Creating a Culture of Cybersecurity

CGFOA Virtual Events

CGFOA

Introductions

Kyle Miller, CISSP, CISA, CDPSE, QSA

Principal, Cybersecurity Consulting

Kyle has over a decade of cybersecurity auditing and consulting experience. He also has experience providing IT system implementation, maintenance, and support in a higher education environment. Kyle's current focus is in providing cybersecurity related audit and consulting services to clients in the public sector where he serves as Plante Moran's cybersecurity industry champion. He serves as a trusted advisor to many state and local governments, airport, transit agencies, special districts, higher education, and K-12 organizations. Kyle focus is in interpreting various information security related standards, frameworks, and regulations (e.g., NIST, CIS, PCI DSS, GLBA, CJIS, FERPA, HIPAA, etc.) and helping organizations understand their overall risk to establish prioritized roadmaps to address that risk. Kyle's professional certifications include the Certified Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Data Privacy Solutions Engineer (CDPSE), and Qualified Security Assessor (QSA).

What are we doing here?!

Agenda:

- The state of cyber for the public sector
- Steps to establishing a culture of cybersecurity
- Quick wins for cyber defense
- Cyber funding opportunities
- Question & Answers

The state of cybersecurity for the public sector

Is it all doom and gloom?!?

2025 Verizon DBIR Data

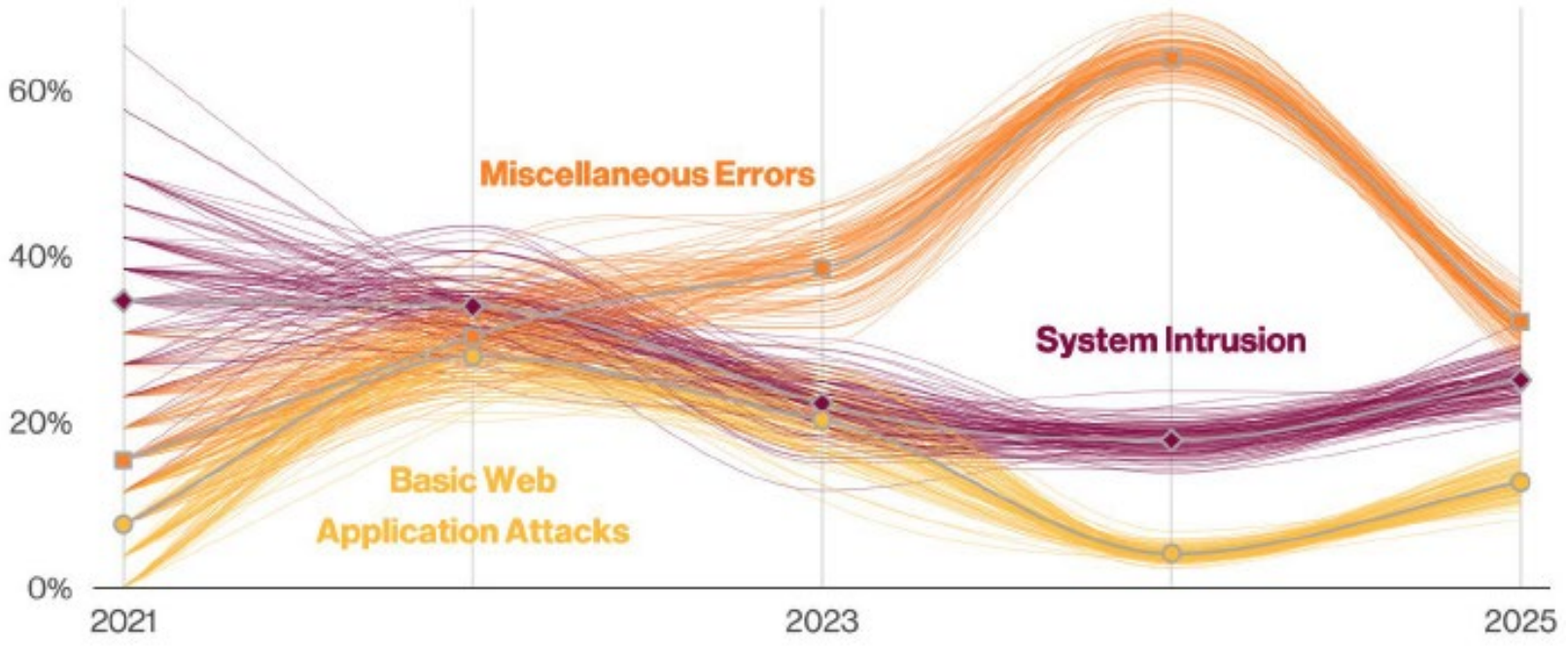
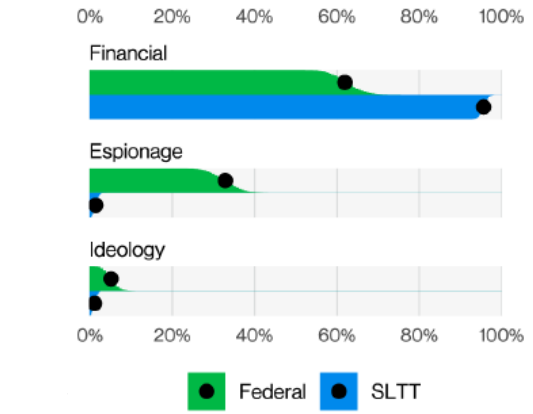


Figure 97. Top patterns over time in SLTT Public Sector breaches

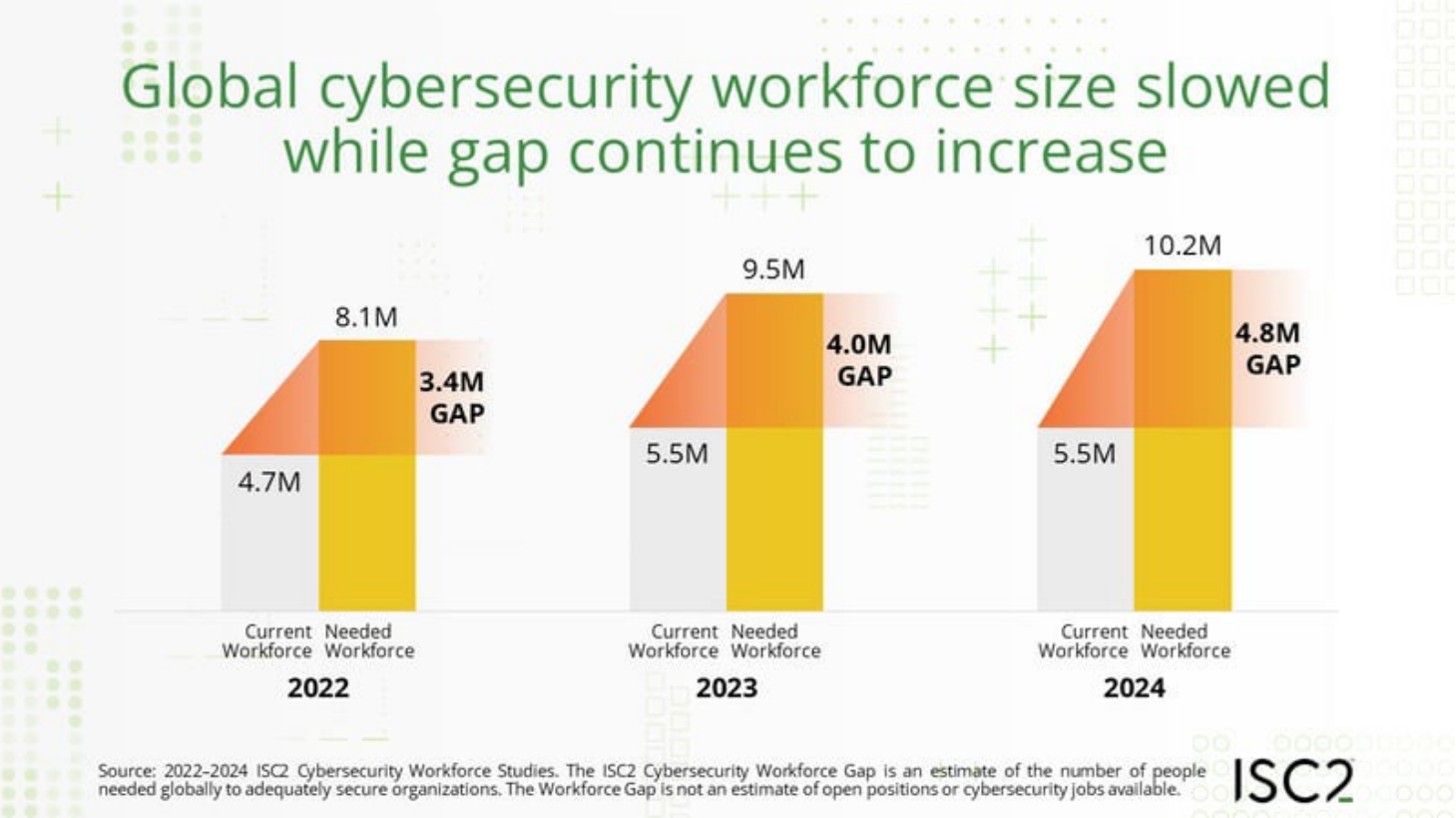
State, Local, Territorial and Tribal (SLTT)

Frequency	2,101 incidents, 1,341 with confirmed data disclosure
Top patterns	Miscellaneous Errors, System Intrusion and Basic Web Application Attacks represent 79% of breaches
Threat actors	External (55%), Internal (45%), Partner (1%) (breaches)
Actor motives	Financial (96%), Espionage (1%), Ideology (1%), Convenience (1%) (breaches)
Data compromised	Personal (83%), Other (29%), Internal (21%), Credentials (12%) (breaches)

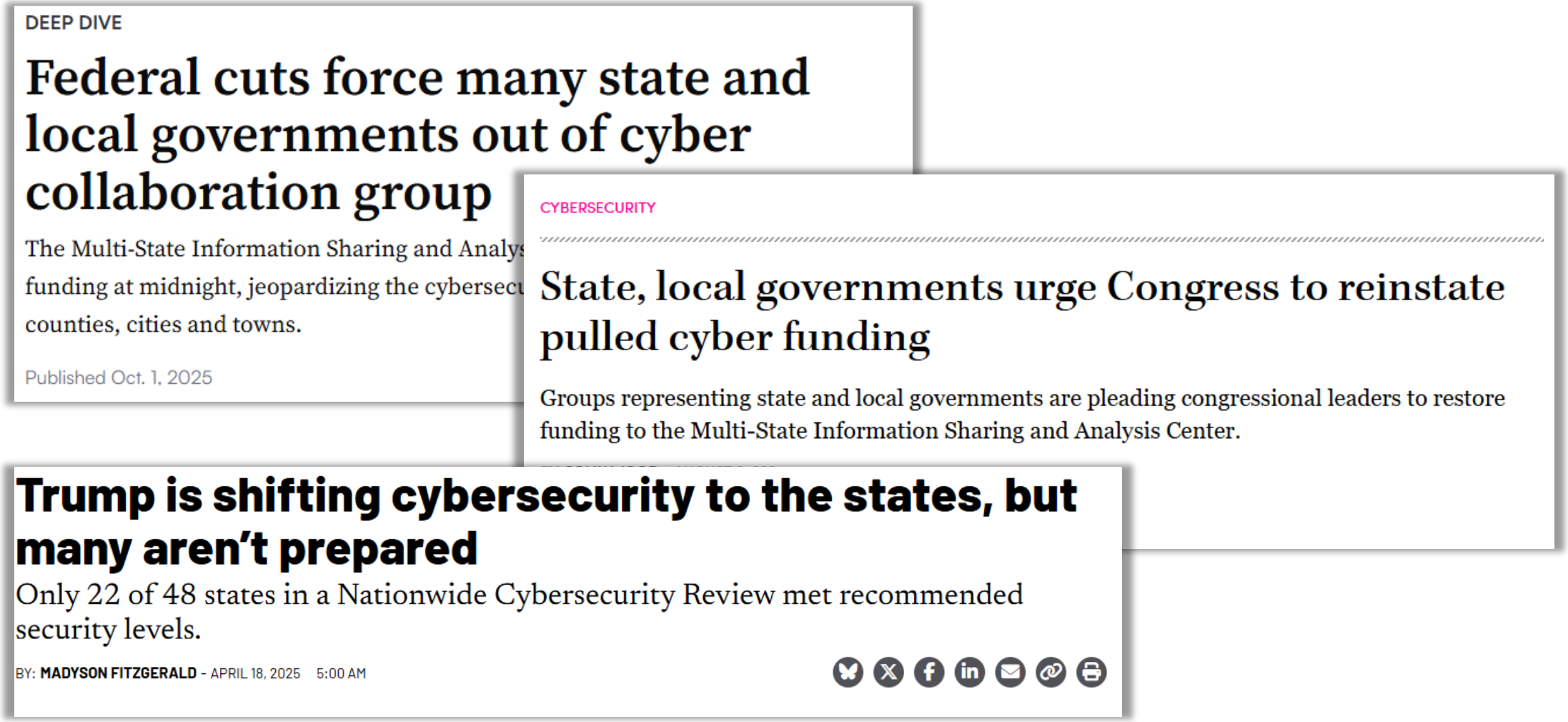


SOURCE: 2025 Data Breach Investigation Report (Verizon)

Cyber workforce concerns



Funding concerns



DEEP DIVE

Federal cuts force many state and local governments out of cyber collaboration group

The Multi-State Information Sharing and Analys
funding at midnight, jeopardizing the cybersecu
counties, cities and towns.

Published Oct. 1, 2025

CYBERSECURITY

State, local governments urge Congress to reinstate pulled cyber funding

Groups representing state and local governments are pleading congressional leaders to restore funding to the Multi-State Information Sharing and Analysis Center.

Trump is shifting cybersecurity to the states, but many aren't prepared

Only 22 of 48 states in a Nationwide Cybersecurity Review met recommended security levels.

BY: **MADYSON FITZGERALD** - APRIL 18, 2025 5:00 AM

What can we do?

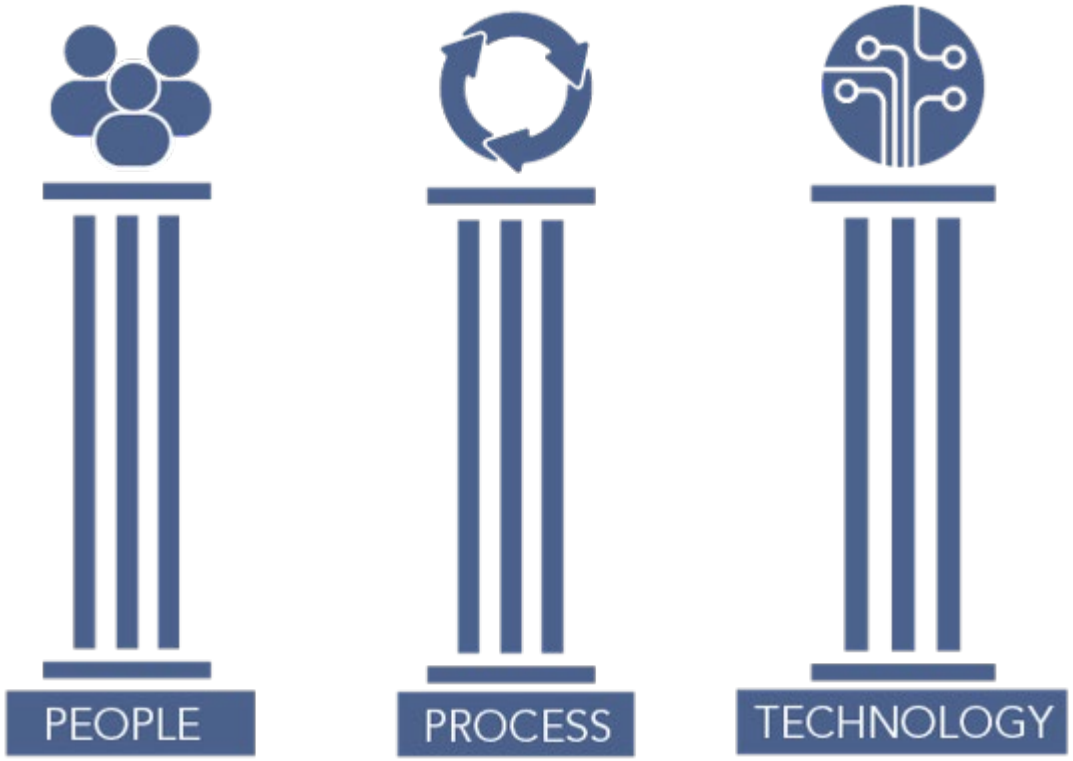
Steps to creating a culture of cybersecurity

- Establish a culture of security
- Select and support a "Security Program Manager"
- Review and approve an incident response plan
- Participate in table top exercises and drills
- Supporting IT leaders

Steps to establishing a culture of cybersecurity

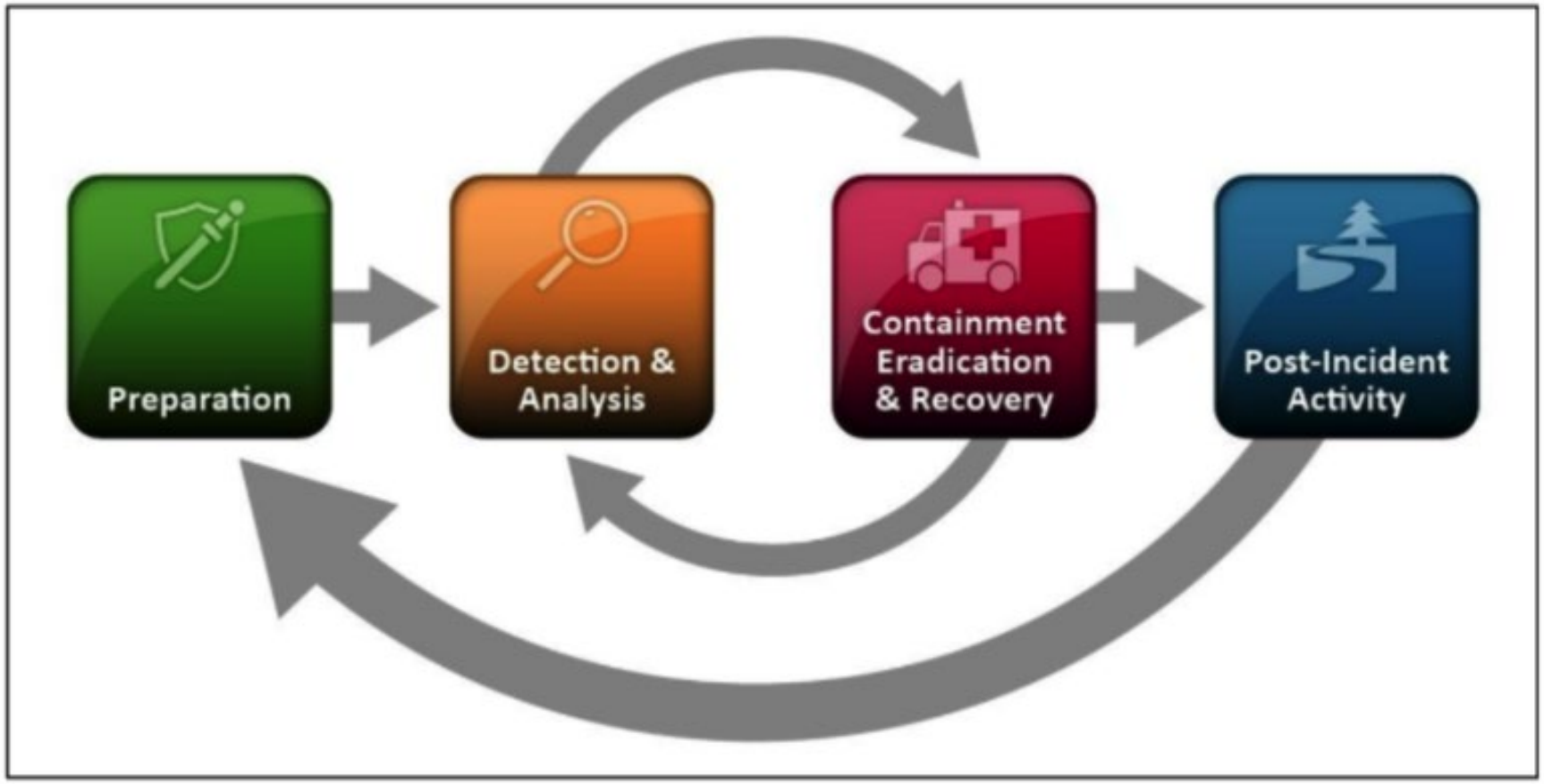
Establishing a culture of security

- Accept that cybersecurity is NOT just an IT issue
- Tone at the top
- Integrate into business as usual
- Test and remind often



Selecting and supporting a “Security Program Manager”

Reviewing and approving the IRP



Participating in tabletop exercises

- Tabletop exercises should include a cross-functional representation from all departments.
- Incident response team members should syndicate knowledge to the staff they are responsible for.

Supporting IT leaders

Quick wins for cyber defense

Top recommended countermeasures

- Implement multi-factor authentication
- Identify and fix known security flaws
- Perform and test backups
- Develop an incident response plan
- Minimize external exposures
- Create security awareness training at all levels

Continue maturing your program

High priority security controls
6 “controls”

CISA cybersecurity performance goals
38 “goals”

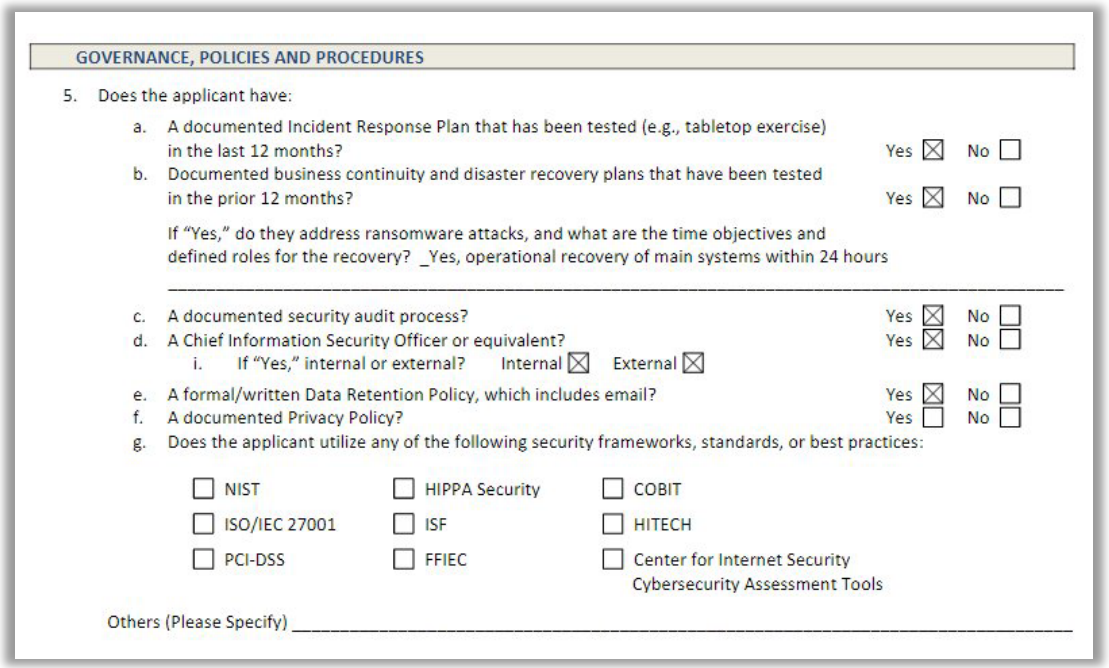
NIST Cybersecurity Framework
109 “subcategories”

Cyber insurance

Per the GFOA Center for Digital Government Cyber Risk Savvy | How to be a Smart Customer of Cyber Insurance:

- Know the basics of your cybersecurity situation
- Quantify your risk
- Examining the potential for insurance
- Periodically reassessing your situation

A friendly reminder on cyber insurance…



GOVERNANCE, POLICIES AND PROCEDURES

5. Does the applicant have:
   a. A documented Incident Response Plan that has been tested (e.g., tabletop exercise) in the last 12 months? Yes ☒ No ☐
   b. Documented business continuity and disaster recovery plans that have been tested in the prior 12 months? Yes ☒ No ☐

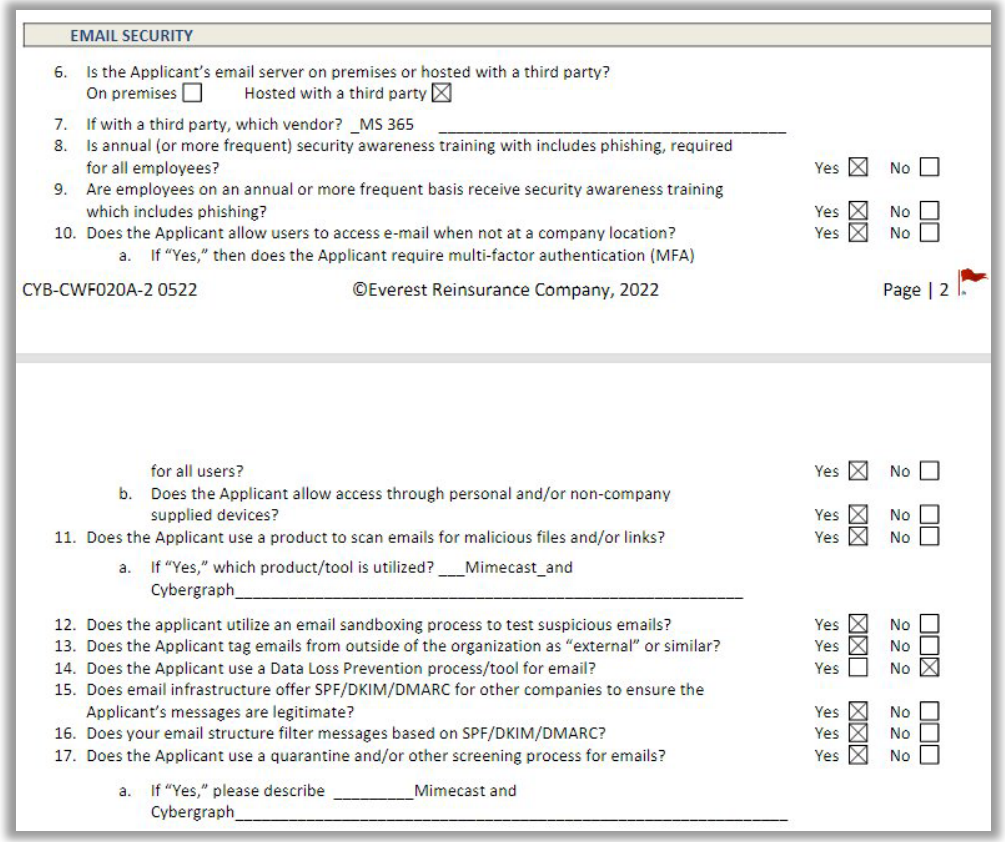
      If "Yes," do they address ransomware attacks, and what are the time objectives and defined roles for the recovery? _Yes, operational recovery of main systems within 24 hours

      _____

   c. A documented security audit process? Yes ☒ No ☐
   d. A Chief Information Security Officer or equivalent? Yes ☒ No ☐
      i. If "Yes," internal or external? Internal ☒ External ☒
   e. A formal/written Data Retention Policy, which includes email? Yes ☒ No ☐
   f. A documented Privacy Policy? Yes ☐ No ☐
   g. Does the applicant utilize any of the following security frameworks, standards, or best practices:

☐ NIST	☐ HIPPA Security	☐ COBIT
☐ ISO/IEC 27001	☐ ISF	☐ HITECH
☐ PCI-DSS	☐ FFIEC	☐ Center for Internet Security Cybersecurity Assessment Tools

Others (Please Specify) _____



EMAIL SECURITY

6. Is the Applicant's email server on premises or hosted with a third party?
   On premises ☐ Hosted with a third party ☒
7. If with a third party, which vendor? _MS 365 _____
8. Is annual (or more frequent) security awareness training with includes phishing, required for all employees? Yes ☒ No ☐
9. Are employees on an annual or more frequent basis receive security awareness training which includes phishing? Yes ☒ No ☐
10. Does the Applicant allow users to access e-mail when not at a company location? Yes ☒ No ☐
    a. If "Yes," then does the Applicant require multi-factor authentication (MFA) for all users? Yes ☒ No ☐
    b. Does the Applicant allow access through personal and/or non-company supplied devices? Yes ☒ No ☐
11. Does the Applicant use a product to scan emails for malicious files and/or links? Yes ☒ No ☐
    a. If "Yes," which product/tool is utilized? ___Mimecast_and Cybergraph_____
12. Does the applicant utilize an email sandboxing process to test suspicious emails? Yes ☒ No ☐
13. Does the Applicant tag emails from outside of the organization as "external" or similar? Yes ☒ No ☐
14. Does the Applicant use a Data Loss Prevention process/tool for email? Yes ☐ No ☒
15. Does email infrastructure offer SPF/DKIM/DMARC for other companies to ensure the Applicant's messages are legitimate? Yes ☒ No ☐
16. Does your email structure filter messages based on SPF/DKIM/DMARC? Yes ☒ No ☐
17. Does the Applicant use a quarantine and/or other screening process for emails? Yes ☒ No ☐
    a. If "Yes," please describe _____Mimecast and Cybergraph_____

CYB-CWF020A-2 0522 ©Everest Reinsurance Company, 2022 Page | 2

Cyber funding opportunities

Funding opportunities

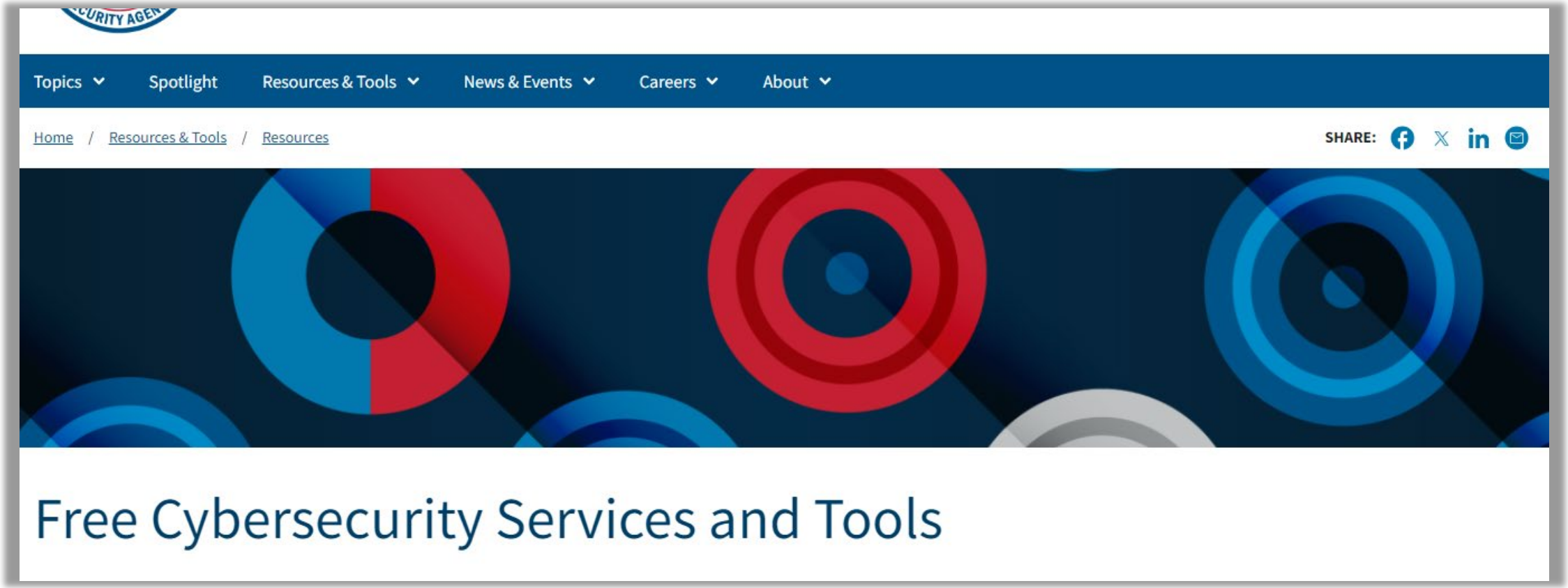
Colorado State and Local Cybersecurity Grant Program

- $6.55 million in funding in 2023 to Colorado
- Annual application process starting usually in May

Homeland Security Grant Program

- Dedicates 7.5% of funds ($75.6 million in FY2024) to support critical infrastructure cybersecurity
- Application through Grants.gov as opportunities arise

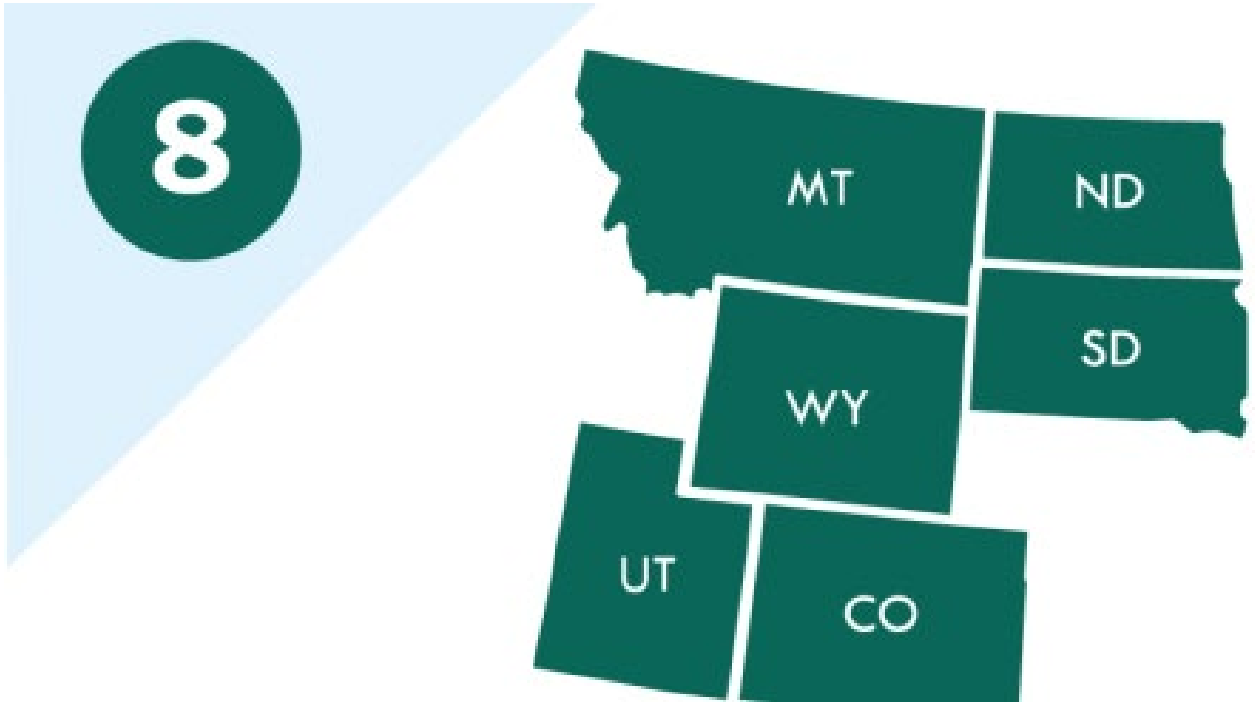
Low-cost services



Ask more of tech providers

Where a local government organization identifies a technology that is not meeting expectations for security built-in, contact your regional cybersecurity advisor to begin a conversation on how we can help.

You are in CISA region 8!



Minimize the burden of on-premises security

Kyle Miller
Principal, Cybersecurity
kyle.miller@plantemoran.com
303.846.3518