



# Cyber Trends and Best Practices

Maria S. Thompson

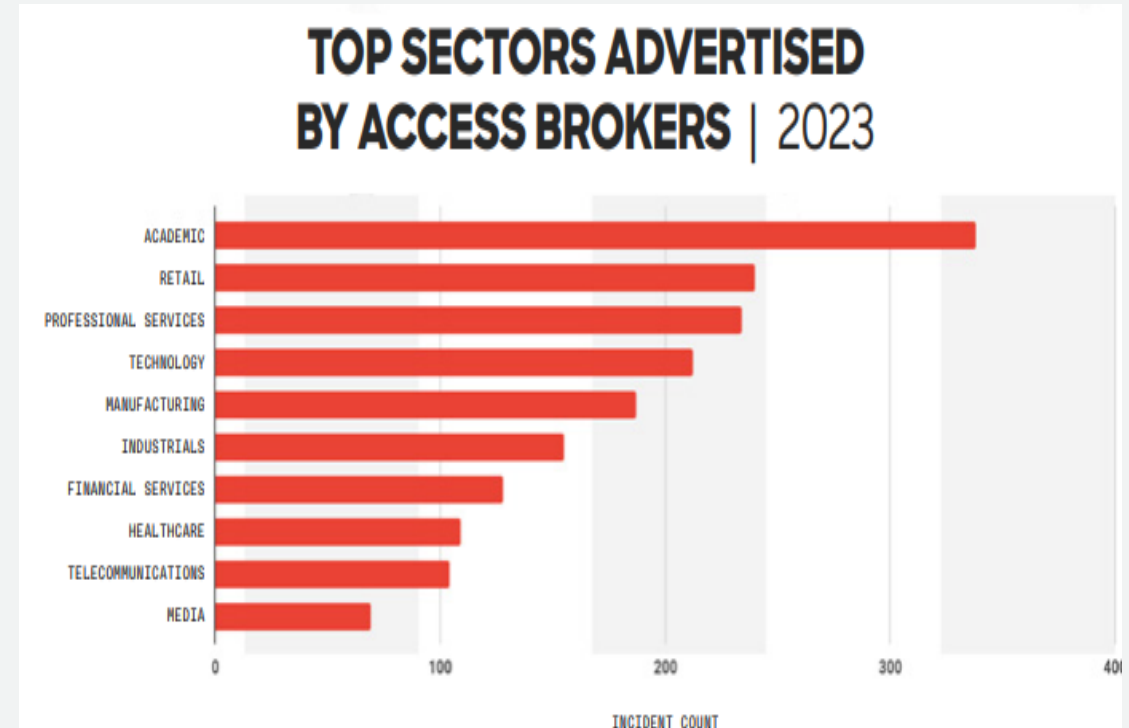
SLG Executive Govt Advisor – Cybersecurity  
AWS

# AGENDA

- Cyber Threat Landscape
- Challenges & Threats facing Public Sector & Academia
- Prevalence of Cyber attacks
- Cyber Legislative Trends
- Why the Cloud?
- Opportunities for success
- Parting Advice

# Cyber Threat Landscape

- Identity-based attacks on the rise
- 34 new threat actors
- 20% increase in Access Brokers
- Breakout time decreased from 84 minutes to **62 minutes in 2023**
- Fastest breakout time 2 mins & 7 seconds



Source: CrowdStrike 2024 Global Threat Report

# Challenges & Threats facing Public Sector

- Compliance requirements
- Lack of data / IT strategy
- Workforce shortages
- Legacy Infrastructure
- Increase in connected devices
- Insecure systems
- Lack of security as a culture mindset
- Third party risks
- Emerging threats

COUNTY & LOCAL

## Ransomware attack forces Colorado public defenders to disable network

A cyberattack led the Colorado State Public Defender's office to shut down its network — the latest in a string of incidents disrupting local court systems.

BY SOPHIA FOX-SOWELL • FEBRUARY 12, 2024

## JeffCo Schools hacker demands money, threatens to release stolen data

Nicole C. Brambila nico.brambila@denvergazette.com Nov 10, 2023 Updated Nov 30, 2023

LOCAL NEWS >

## Colorado Department of Higher Education hit by ransomware attack

CBS NEWS  
COLORADO

By Logan Smith  
August 6, 2023 / 2:10 PM MDT / CBS Colorado



Security

## Colorado warns hackers stole 16 years of public school data in ransomware attack

# Prevalence of Cyber Attacks

- Average total cost of a breach is \$4.45M
- 51% of organizations are planning to increase security investments
- AI and automation is reported to save organizations \$1.76 million in data breach costs
- Healthcare industry data breach costs have increased by 53.3%
- DevSecOps, IR Training and testing reduce cost of a breach

Source: 2023 IBM Cost of a Data Breach Report

Total cost of a data breach

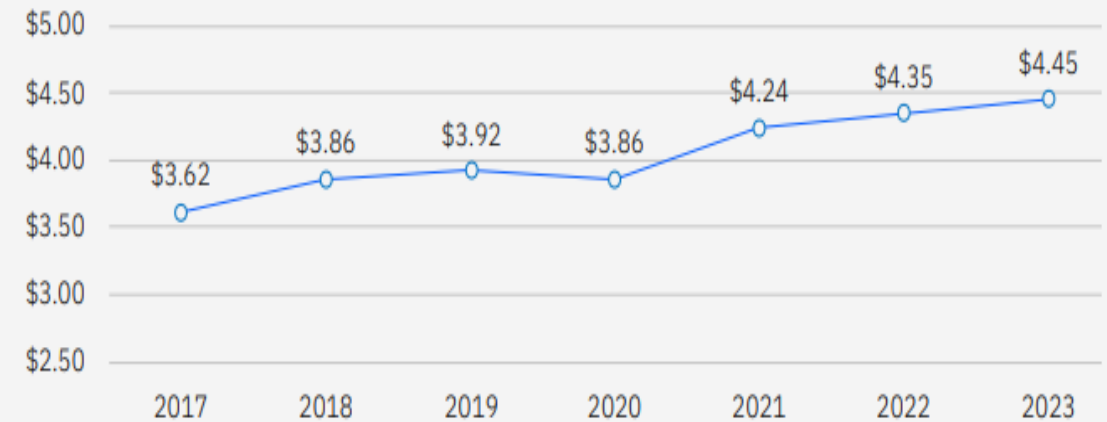


Figure 1. Measured in USD millions

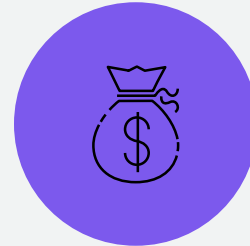
# Ransomware is a growing business risk – Impact to Cyber Insurance

By 2025, 75% of all IT organizations will face one or more ransomware threats (Gartner, 2021).



Increased Incident Rates & Sophistication Levels

---



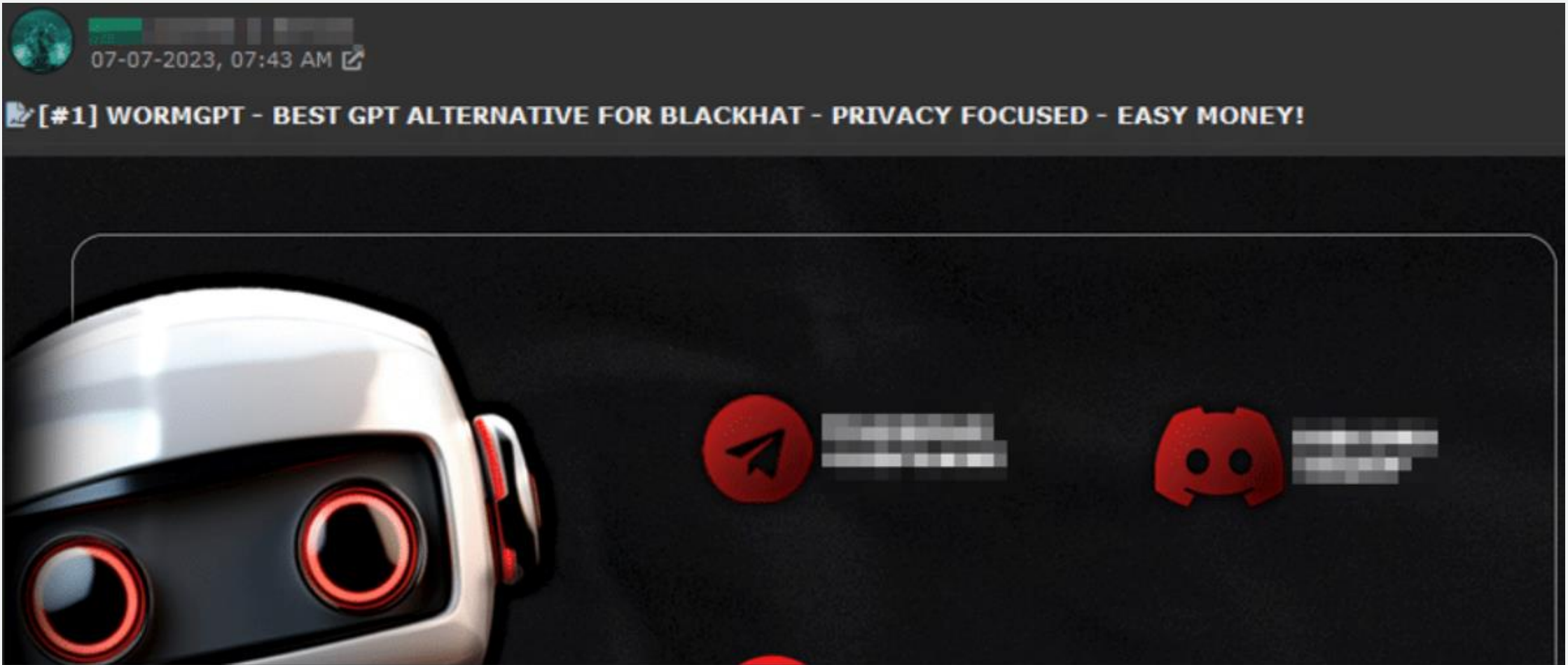
Recovery Costs Skyrocketing

---



Significant Business Impact

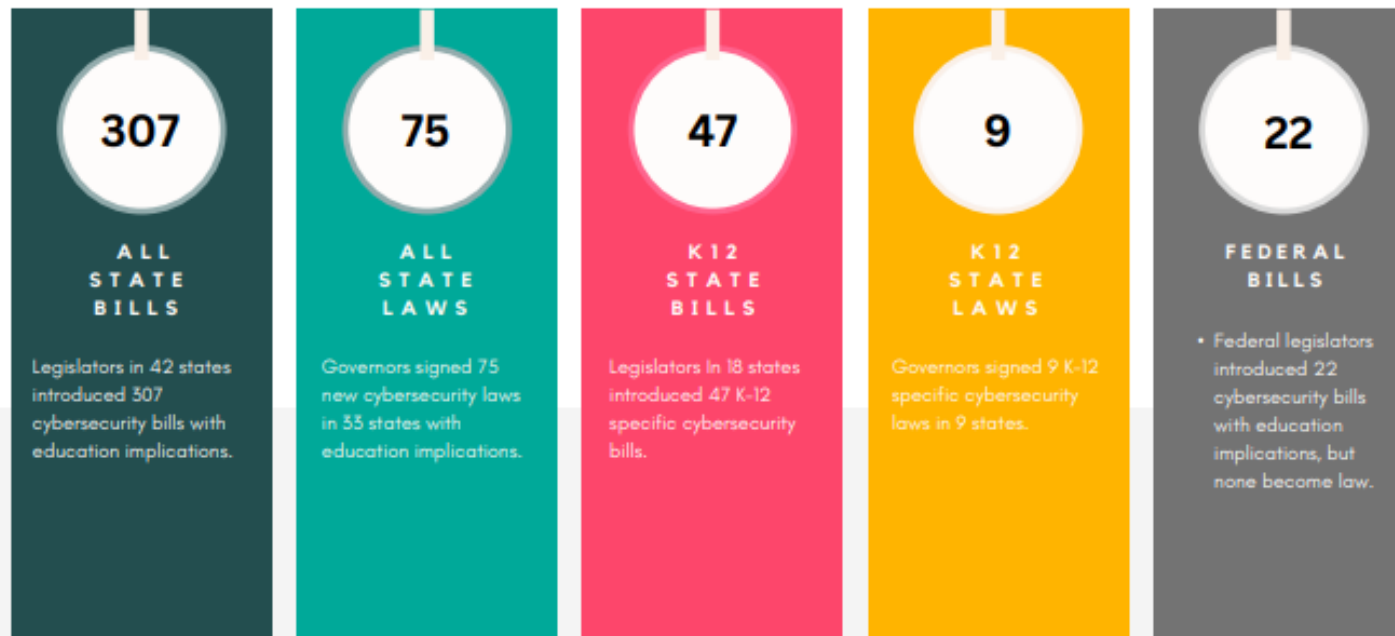
# Prevalence of Cyber Attacks – WormGPT Anyone?



Source: Krebs on Security: Meet the Brains Behind the Malware-Friendly AI Chat Service 'WormGPT'

# Cybersecurity Legislation Trends

## 2023 EDUCATION CYBERSECURITY BILLS & LAWS

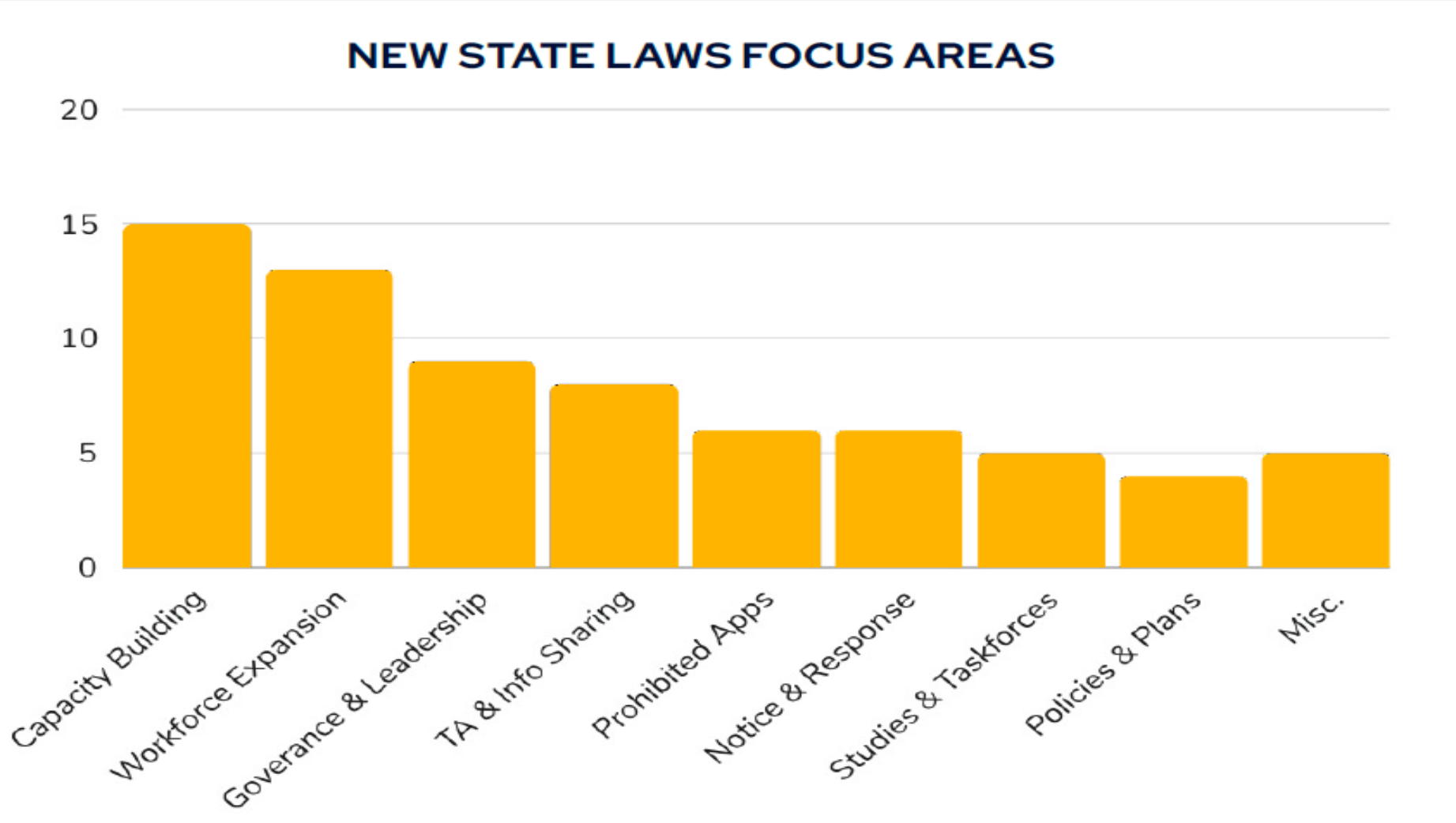




# Cybersecurity Legislation Trends


- **Cyber risk insurance funds:** States created these funds for school districts to mitigate increasing insurance costs
- **Regional alliances and partnerships:** Momentum has grown behind partnerships to promote information sharing and collaborative responses to cybersecurity incidents
- **Cybersecurity workshop expansion:** Scholarship programs have been established to address the shortage of qualified cybersecurity experts
- **Governance enhancement:** Efforts have been made to bolster governance structures to consolidate responsibility and promote prevention and response mechanisms across agencies
- **Cybersecurity task forces:** Several task forces have been established to study and evaluate the cybersecurity landscape, including how artificial intelligence impacts the field


# Cybersecurity Legislation Trends





Source: CoSN - Summary of Education Cybersecurity Policy Developments in 2023 – Focus Area State Cyber Laws Enacted in 2023


# Cyber Insurance

 Lower/reduced coverage

 Higher Rates

 Mandatory requirements

 Less Cyber Underwriters

 FTC suing non-compliant organizations

## Top Cybersecurity Controls

The key to insurability, mitigation, and resilience

Preparation for the underwriting process:

1. Start early! Without positive responses in the top 5 control categories, coverage offered and insurability may be in question.
2. Evaluate your cybersecurity maturity by completing Marsh's Cyber Self-Assessment – where improvements are needed, leverage [Cyber Catalyst vendors](#).
3. Expect more rigorous underwriting and more detailed questions from underwriters.



Multifactor authentication for remote access and admin/privileged controls



Endpoint Detection and Response (EDR)



Secured, encrypted, and tested backups



Privileged Access Management (PAM)



Email filtering and web security



Patch management and vulnerability management



Cyber incident response planning and testing



Cybersecurity awareness training and phishing testing



Hardening techniques, including Remote Desktop Protocol (RDP) mitigation



Logging and monitoring/network protections

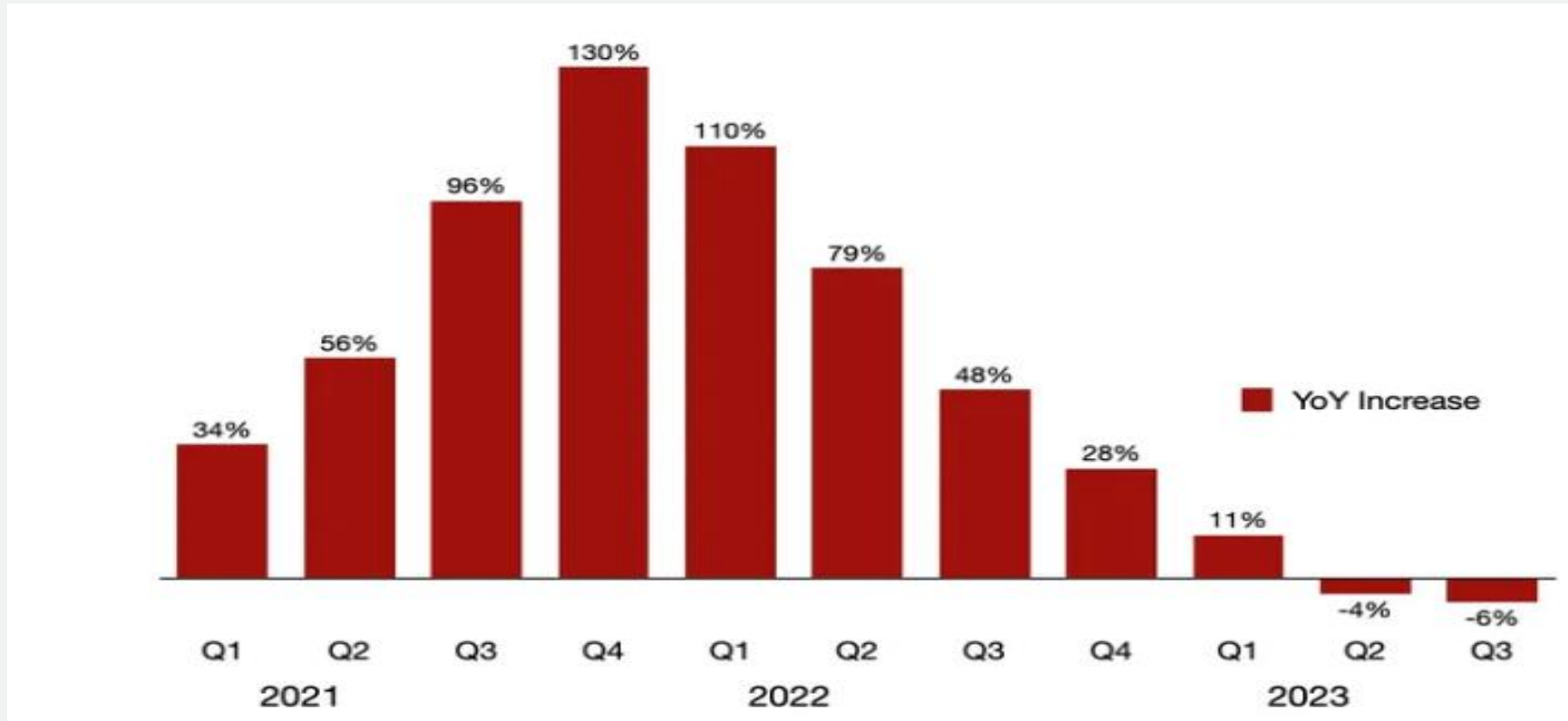


End-of-life systems replaced or protected



Vendor/digital supply chain risk management

# Cyber Insurance Market



## Global insurance markets: Rates continue to stabilize entering 2024

Global commercial insurance rates rose 2% in the fourth quarter of 2023, compared to 3% in the prior two quarters, according to the *Marsh Global Insurance Market Index*. This was the twenty-fifth consecutive quarter in which composite rates rose, continuing the longest run of increases since the inception of the index in 2012.

Source: Marsh Global Insurance Market Index

# AWS Cyber Insurance Partner

Cyber Insurance Partners have committed to generating a quote for AWS customers within 2 business days of the request for a quote. Customers will use external SaaS insurance platforms that provide:

- Direct, easy-quote systems that run an audit of their AWS environments and security posture to provide a cyber insurance quote, including recommended actions that can result in lower rates.
- Ongoing subscription based cyber insurance that moves with the customer based on their assessed security posture and size, allowing customers' coverage to match and grow with them

[AWS Cyber Insurance Partners - Amazon Web Services \(AWS\)](#)

# Recommendations for organizations



Invest in the most impactful security measures



Recognize and actively address resource constraints



Focus on collaboration and information sharing

Source: [Partnering to Safeguard K-12 Organizations from Cybersecurity Threats](#), CISA

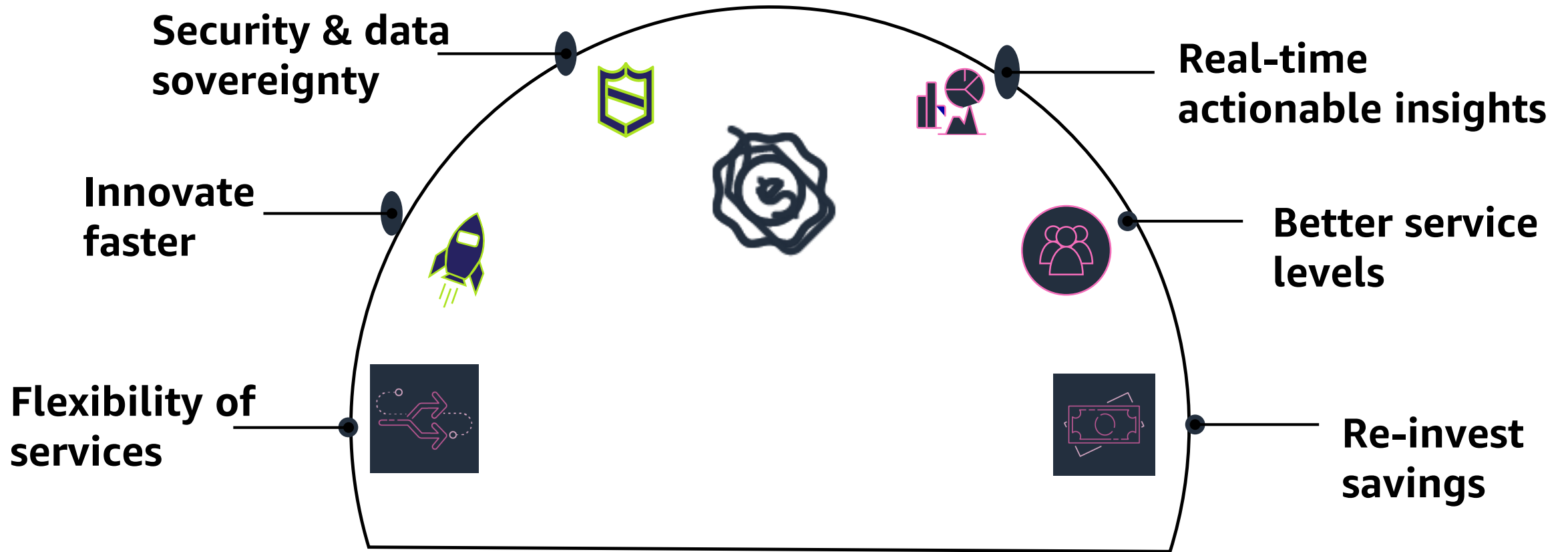
# Cybersecurity Strategies

- Whole of [Insert AOR] Cybersecurity
- Establishing governance models
- Developing cybersecurity strategic plans
- Collaborating across the sector lines
- Focusing on mission areas as priority
- Developing use cases to leverage AI/ML



Fig. 2. CSF Functions

# Why the Cloud - enabler for Digital Transformation





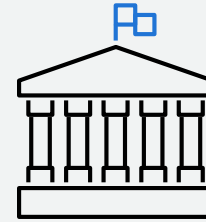
# Why the Cloud - Highest standards for privacy and data security



**Meet data  
residency  
requirements**



**Encryption at scale**

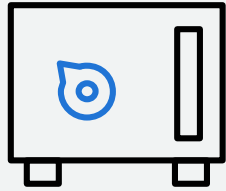


**Comply with local  
data privacy laws**

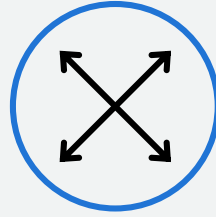


Access services and  
tools that enable you  
to  
**build compliant  
infrastructure**

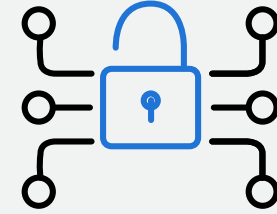
# Why the Cloud - Infrastructure & services to elevate your security



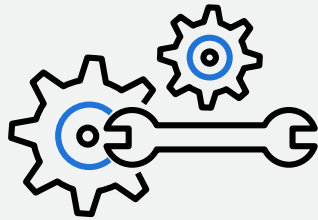
Inherit global security and compliance controls



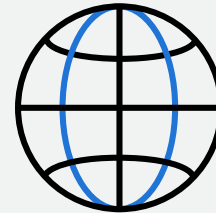
Scale with superior visibility and control



Highest standards for privacy and data security



Automate & reduce risk with deeply integrated services



Largest ecosystem of security partners and solutions

# Why the cloud - Inherit global security and compliance controls



# Imagine if there was a service that...



**Allow for  
State entities  
to procure  
security  
capabilities  
based specific  
cyber gaps**



**Centralizes  
and allows  
Enterprise  
visibility of  
contracts for  
mandatory  
reporting**



**Allows for  
volume  
discounts and  
cost  
optimization**



**Enables  
centralized  
enterprise  
security  
visibility into  
threats across  
the state**

# Opportunities for Success - Re-assess, Reinforce and Reconnect

- ✓ Develop a continuous monitoring plan
- ✓ Prioritize data resilience and modernization
- ✓ Leverage cloud for resiliency and immutable backup capabilities
- ✓ Implement information sharing for collective defense – use “persistent collaboration”
- ✓ Re-assess/review security architecture periodically
- ✓ Use integrated solutions w/automation
- ✓ Leverage federal funding opportunities
- ✓ TEST, TEST and...TEST
- ✓ Revamp procurement processes - create digital catalogs for approved services
- ✓ Apply responsible AI principles to all AI/ML projects



## How do we improve?

CIO/CTO/ CFO/Head of Security, IT Manager, Director of IT Security, Security Operations Manager, Head of Security Architecture

### TOP 3 WAYS

- › Trained and skilled workforce leads to innovation, cultural and behavioral changes
- › Drive growth and reduce risks through IT modernization efforts
- › Take a data centric approach to security and adopting an industry framework for continuous assessment

## Parting Advice: BE SAFE

- B – be collaborative
- E – educate and upskill your teams
- S – secure your data
- A – apply cyber hygiene practices
- F – fund your cyber projects as a lifecycle
- E – everybody is part of the cyber eco-system



# Thank you!

Maria Thompson

thammari@amazon.com

