



Cyber trends and best practices

Maria S. Thompson

SLG Executive Govt Advisor –
Cybersecurity

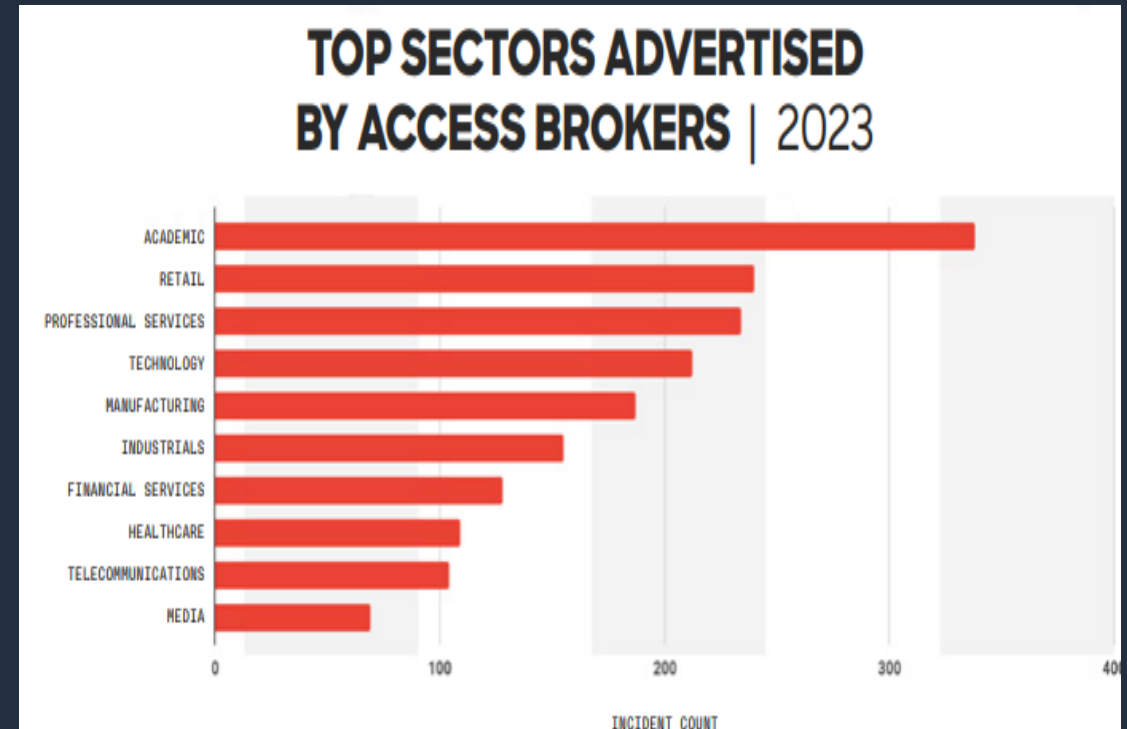
Amazon Web Services

AGENDA

- Cyber threat landscape
- Challenges and threats facing public sector
- 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 percent increase in Access Brokers
- Breakout time decreased from 84 minutes to **62 minutes in 2023**
- Fastest breakout time two minutes and seven seconds



Source: CrowdStrike 2024 Global Threat Report

Challenges and 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

CYBERSECURITY

Ohio city reveals nearly 6,000 affected by recent ransomware attack

A ransomware attack last November compromised the data of nearly 6,000 people, officials in Huber Heights, Ohio, announced this week.

CYBERSECURITY

Ohio's Recent Spate of Cyberattacks Is Indicative of the National Trend

HEALTHCARE

How cyber attacks are crippling Ohio health care systems

[Cole Behrens](#) Columbus Dispatch

Published 11:05 a.m. ET March 7, 2024 | Updated 11:48 a.m. ET March 7, 2024

Ransomware attack on Ohio city impacts multiple services

Prevalence of cyber attacks

- Average total cost of a breach is \$4.45M
- 51 percent 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 percent
- 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

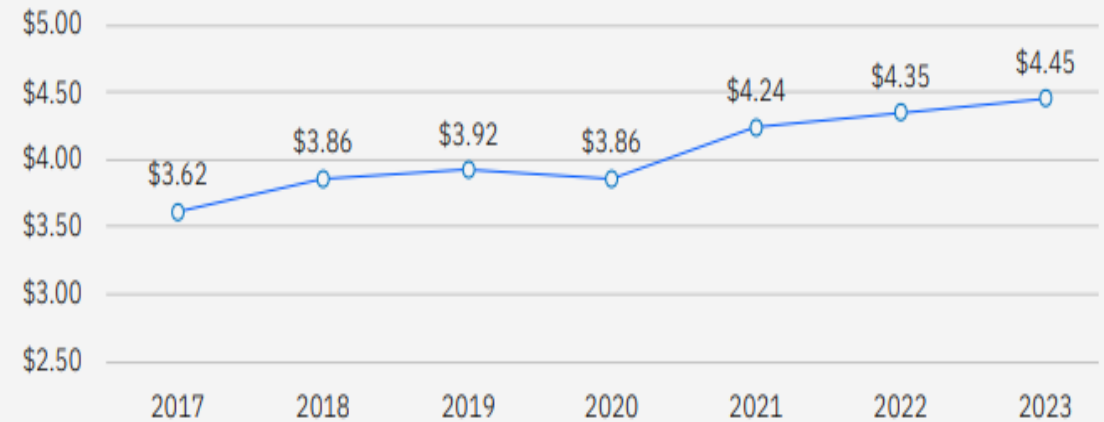


Figure 1. Measured in USD millions

Ransomware is a growing business risk – impact to cyber insurance

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



Increased incident rates and sophistication levels

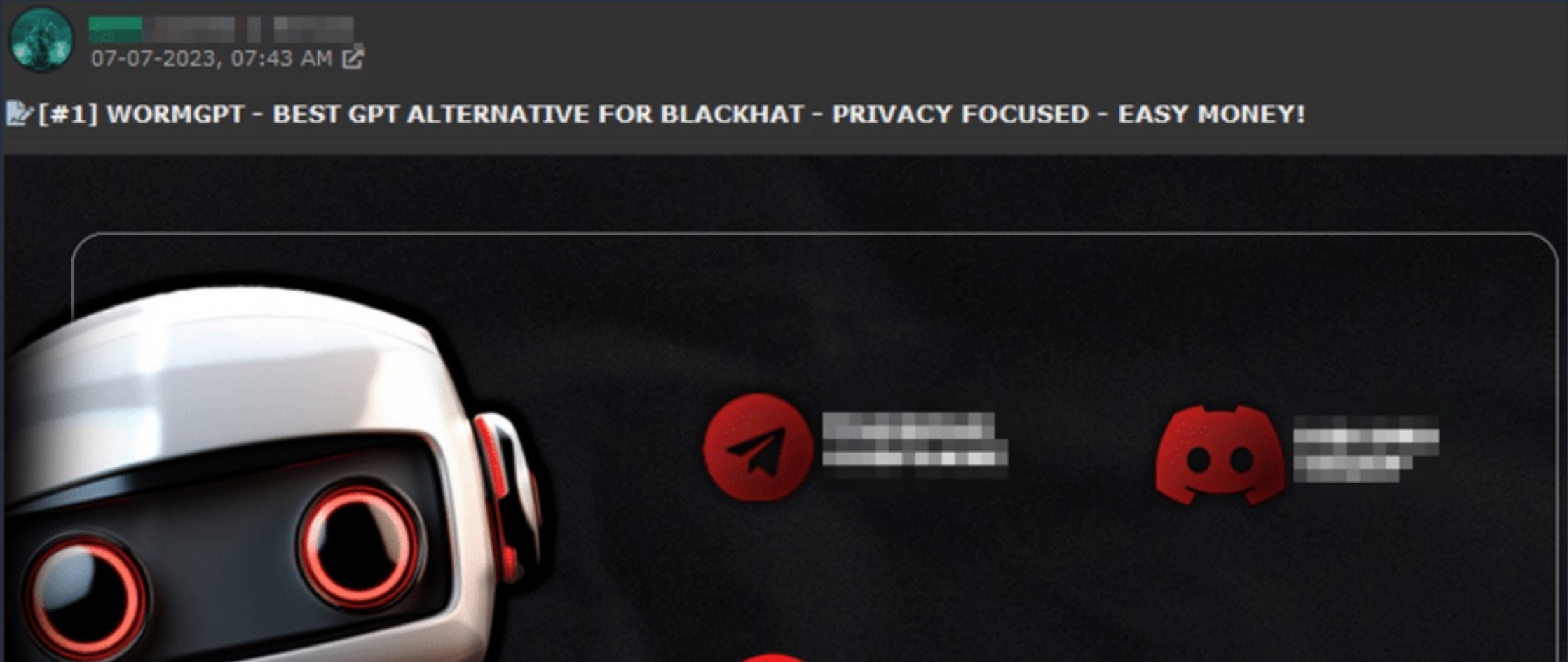


Recovery costs skyrocketing



Significant business impact

Prevalence of cyber attacks – WormGPT anyone?



Source: Krebs on security: Meet the brains behind the malware-friendly AI chat service 'WormGPT'

Risk mitigation strategies

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

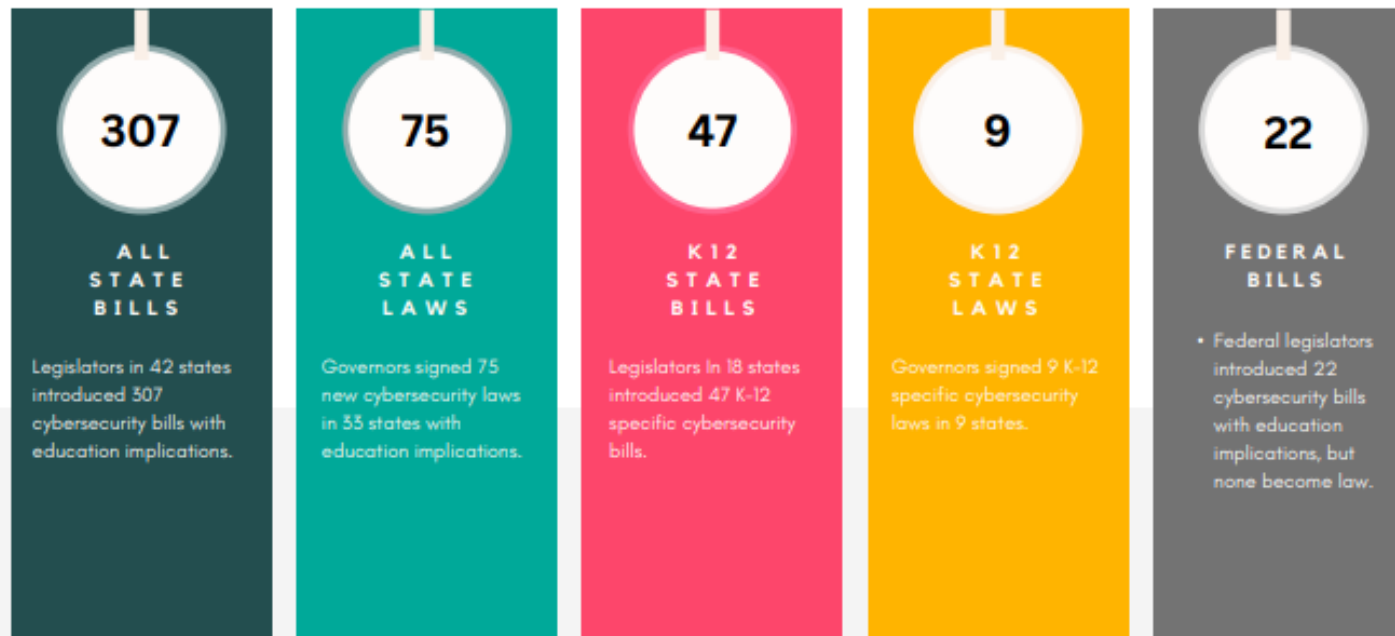
- Whole of [insert AOR] cybersecurity
- Establishing governance models
- Developing cybersecurity strategic plans
- Collaborating across the sector lines
- Focusing on mission areas as priority
- Developing use cases to leverage AI/ML



Fig. 2. CSF Functions

Cybersecurity legislation trends

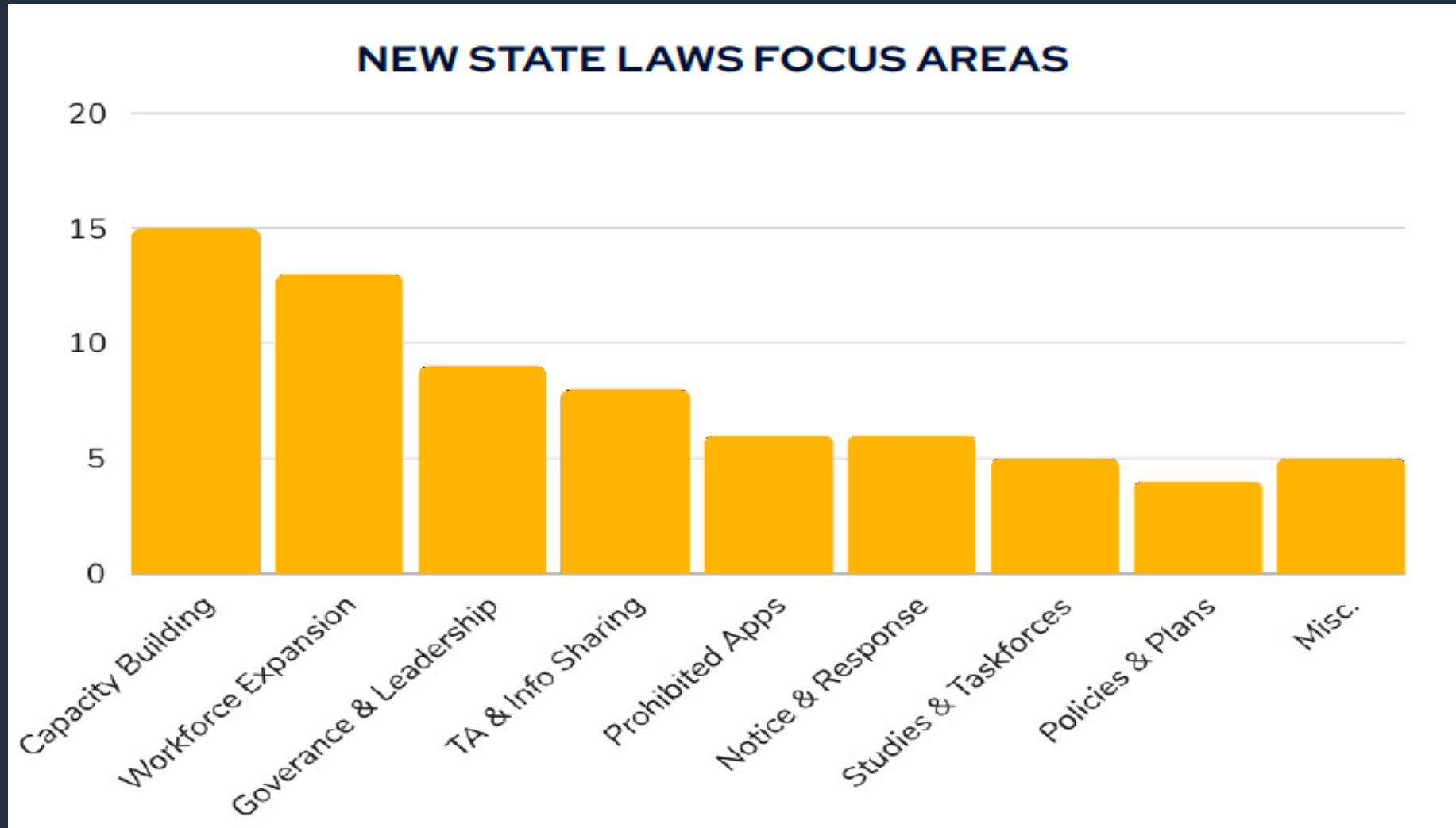
2023 EDUCATION CYBERSECURITY BILLS & LAWS



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

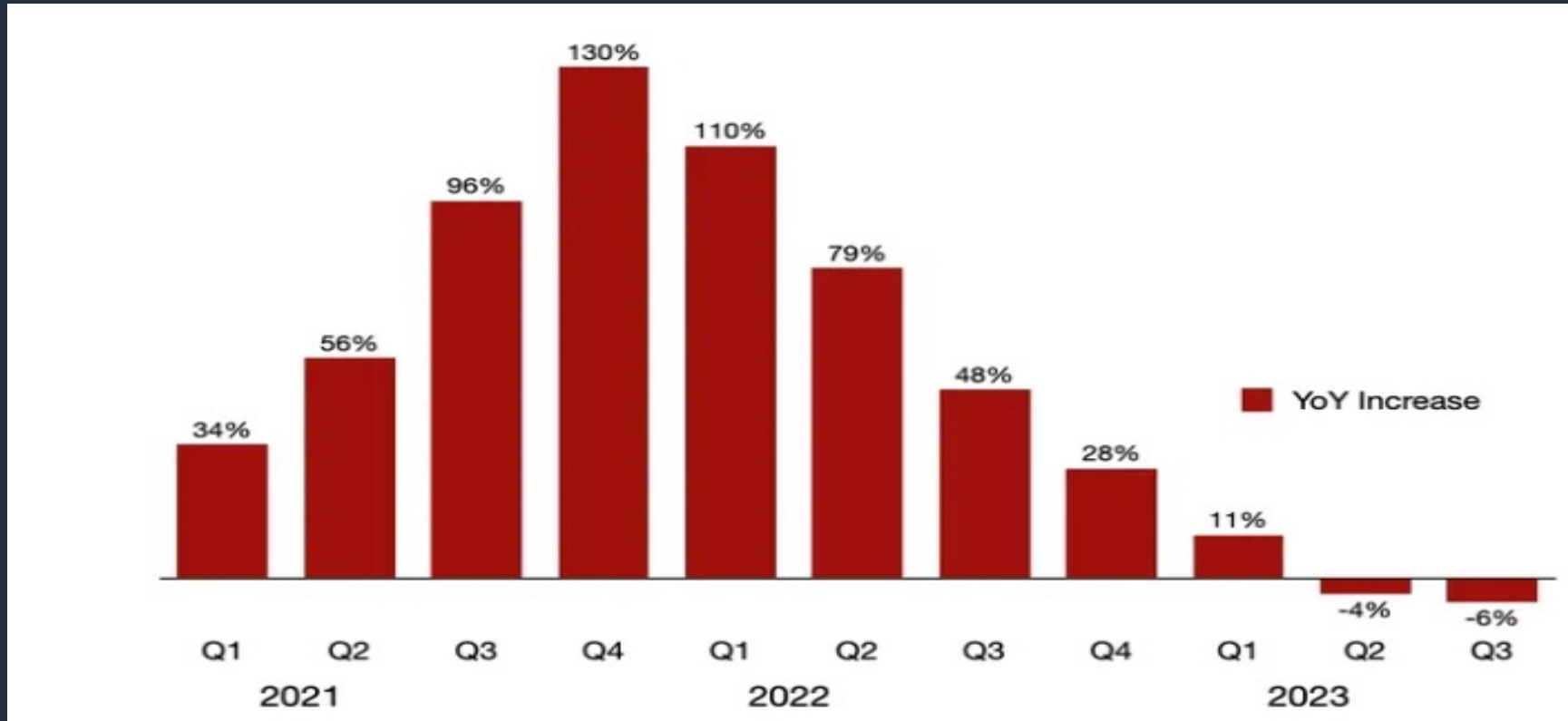


End-of-life systems replaced or protected



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

AWS Cyber Insurance Partners have committed to generating a quote for AWS customers within two 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 \(AWS\)](#)

Think differently – Smart procurement considerations

- Streamline cybersecurity solution procurement to standardize operations and reduce costs
- Find ready-made solutions in a digital catalog to support cybersecurity governance and more
- Prioritize resilience for your infrastructure
- Skill your organization with no-cost cybersecurity training
- Think long-term with a modernization strategy

Source: [5 things to consider while applying to the State and Local Cybersecurity Grant Program \(SLCGP\) | AWS Public Sector Blog \(amazon.com\)](#)

Imagine if there was a service that...



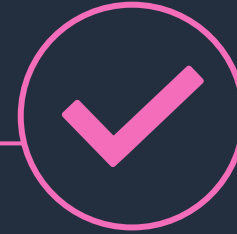
**Allows for
state entities
to procure
security
capabilities
based specific
cyber gaps**



**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**

Why the cloud?



Before...

Move fast

OR

Stay secure

Now... .

Move fast  Stay secure

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 and services to elevate your security



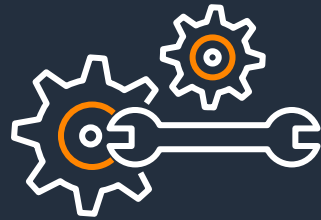
Inherit global security and compliance controls



Scale with superior visibility and control



Highest standards for privacy and data security



Automate and reduce risk with deeply integrated services



Largest ecosystem of security partners and solutions

Why the cloud - Inherit global security and compliance controls



SOC 1



SOC 2



SOC 3



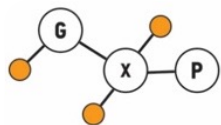
CCCS
PIPEDA



CJIS



FERPA



GxP



MPAA



SEC Rule
17a-4(f)



VPAT
Section 508

FINTECH



FISC



G-Cloud



Cloud is only part of the recipe for success



Organization



Process



Culture

Opportunities for success - Reassess, 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 ecosystem



Thank you!

Maria Thompson



@NC_Cybersec

thammari@amazon.com



Please take our survey: Cyber
trends and best practices