



Cyber trends and best practices

Maria S. Thompson

SLG Executive Govt Advisor –
Cybersecurity

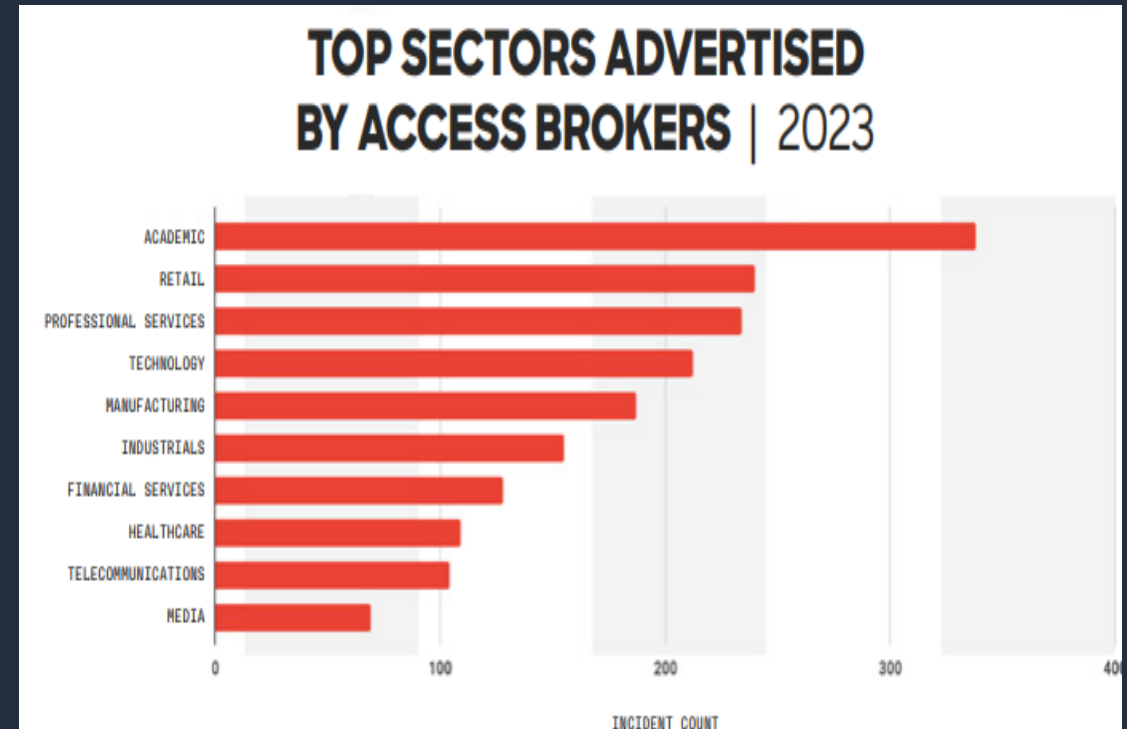
Amazon Web Services

Agenda

- Cyber threat landscape
- Challenges and threats facing public sector
- Cyber legislative trends
- Why the cloud?
- Opportunities for success
- Parting advice

Cyber threat landscape

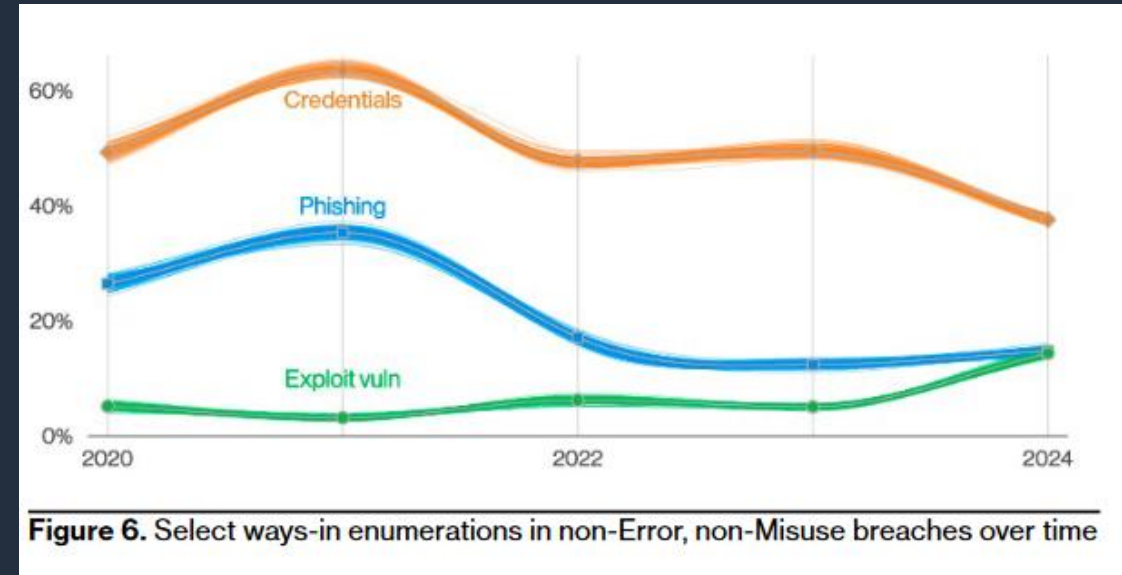
- Identity-based attacks on the rise
- 34 new threat actors
- 20 percent increase in access brokers
- Breakout time decreased from 84 minutes to **62 minutes in 2023**
- Fastest breakout time two minutes and seven seconds



Source: CrowdStrike 2024 Global Threat Report

Cyber threat landscape

- 1/3 of all breaches involved ransomware
- Pure extortion on the rise and is a component of 9 percent all breaches
- Ransomware a top threat across 92 percent of all industries
- 68 percent of breaches involved “human element”
- 15 percent of breaches involved a third-party party



Source: Verizon 2024 Data Breach Investigations 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 technologies and threats

Cybercriminals behind Los Angeles Unified School District ransomware attack release hacked data, superintendent says

CYBERSECURITY

L.A. Housing Authority May Have Fallen Victim to Ransomware

UCLA

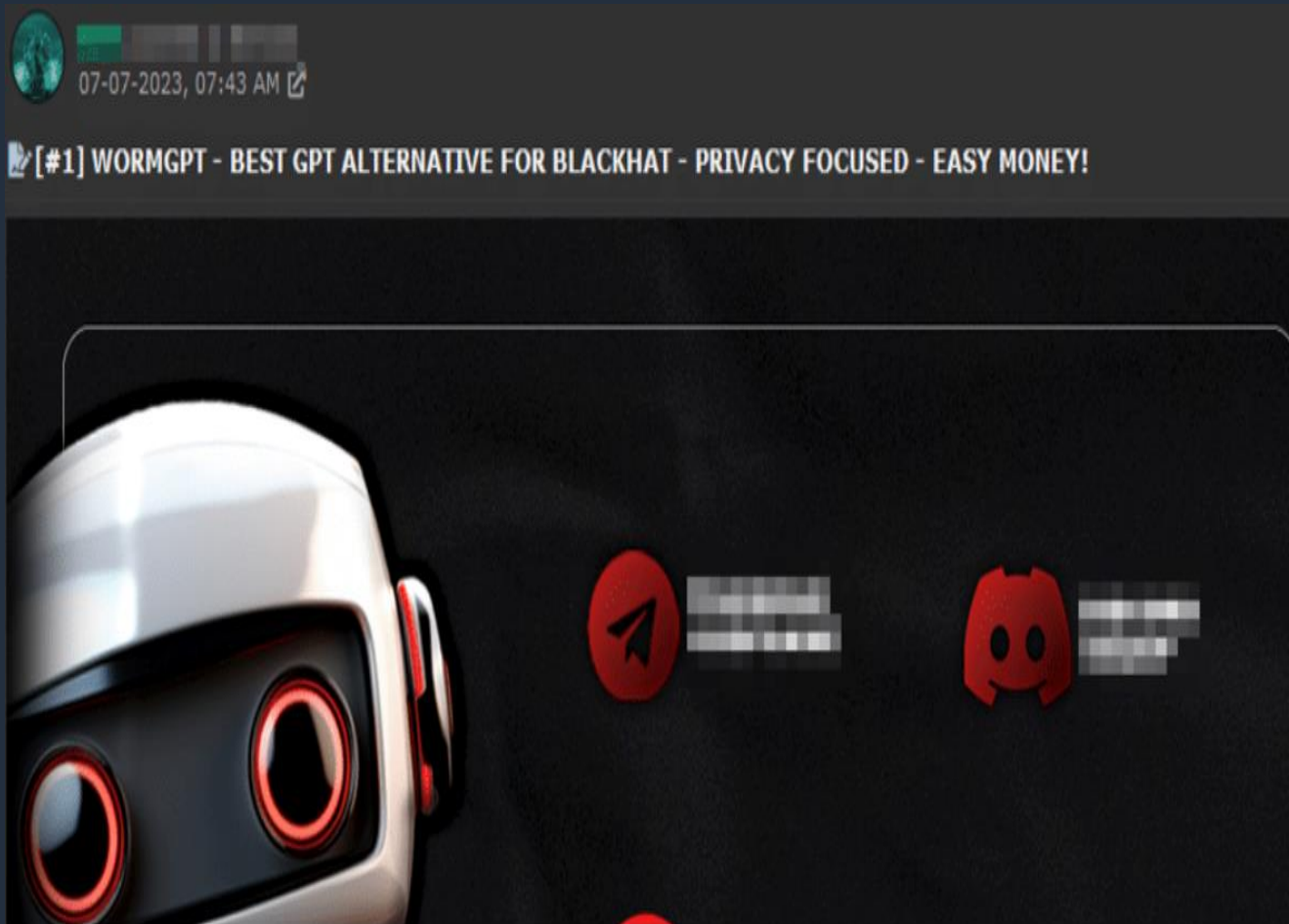
UCLA among victims of worldwide cyber attack

UCLA confirmed this week it is among dozens of institutions and businesses affected by a worldwide cyber theft.

MONEYWATCH

Cyberattack causes multiple hospitals to shut emergency rooms and divert ambulances

Prevalence of cyber attacks – WormGPT anyone?



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

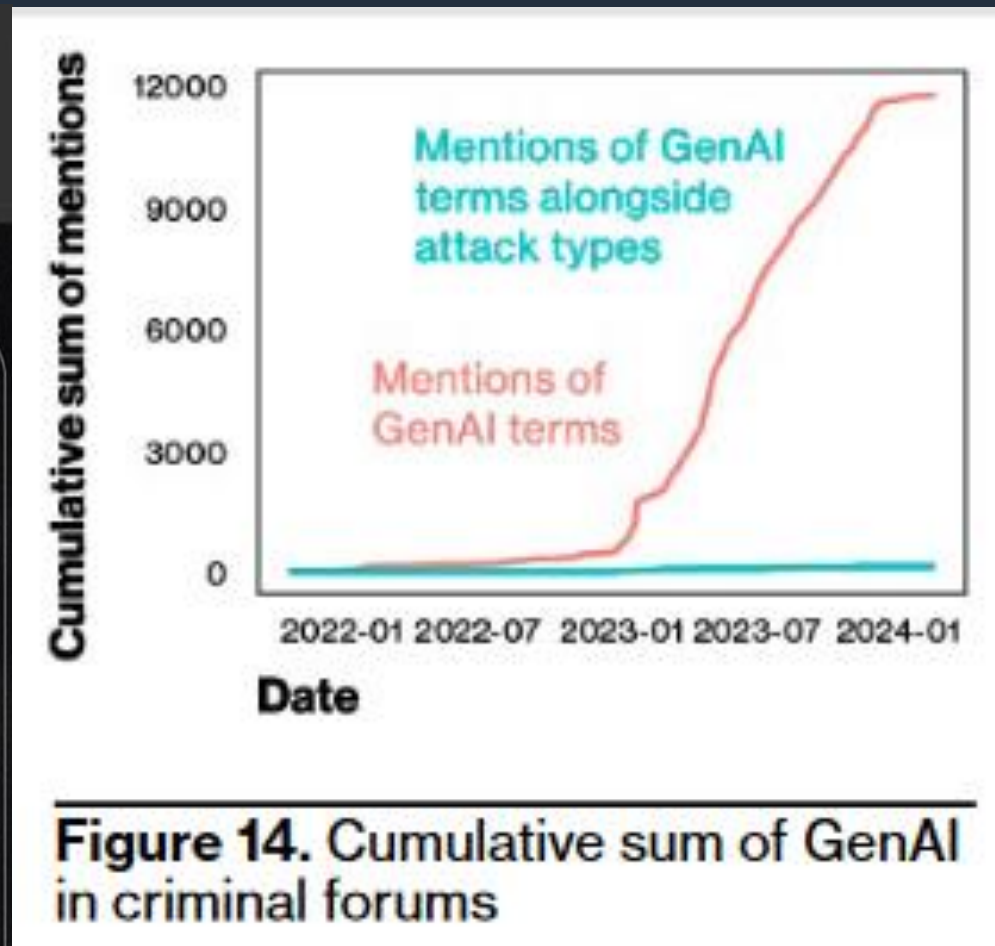


Figure 14. Cumulative sum of GenAI in criminal forums

Source: Verizon 2024 Data Breach Investigations Report

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

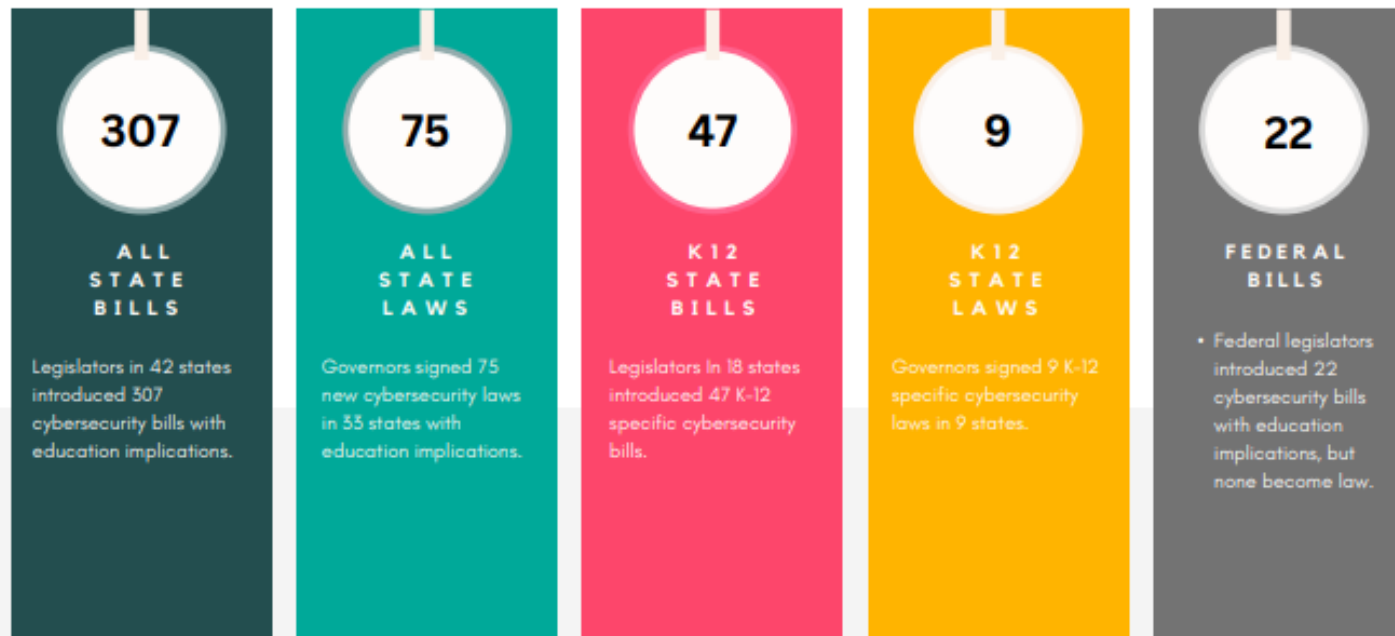
- Whole of [insert AOR] cybersecurity
- Establishing governance models
- Developing cybersecurity strategic plans
- Collaborating across the sector lines
- Focusing on mission areas as priority
- Developing use cases to leverage AI/ML



Fig. 2. CSF Functions

Cybersecurity legislation trends

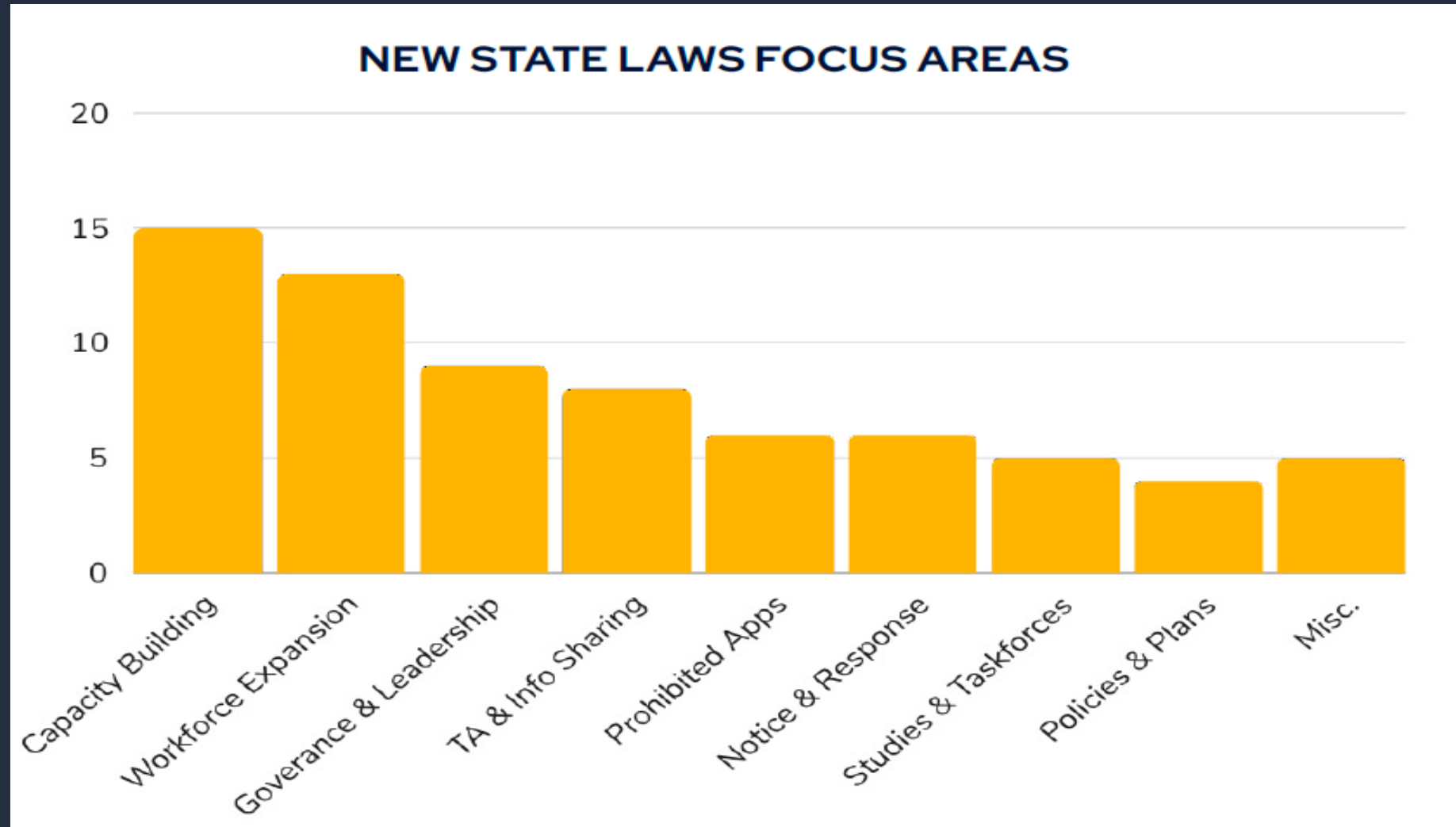
2023 EDUCATION CYBERSECURITY BILLS & LAWS



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

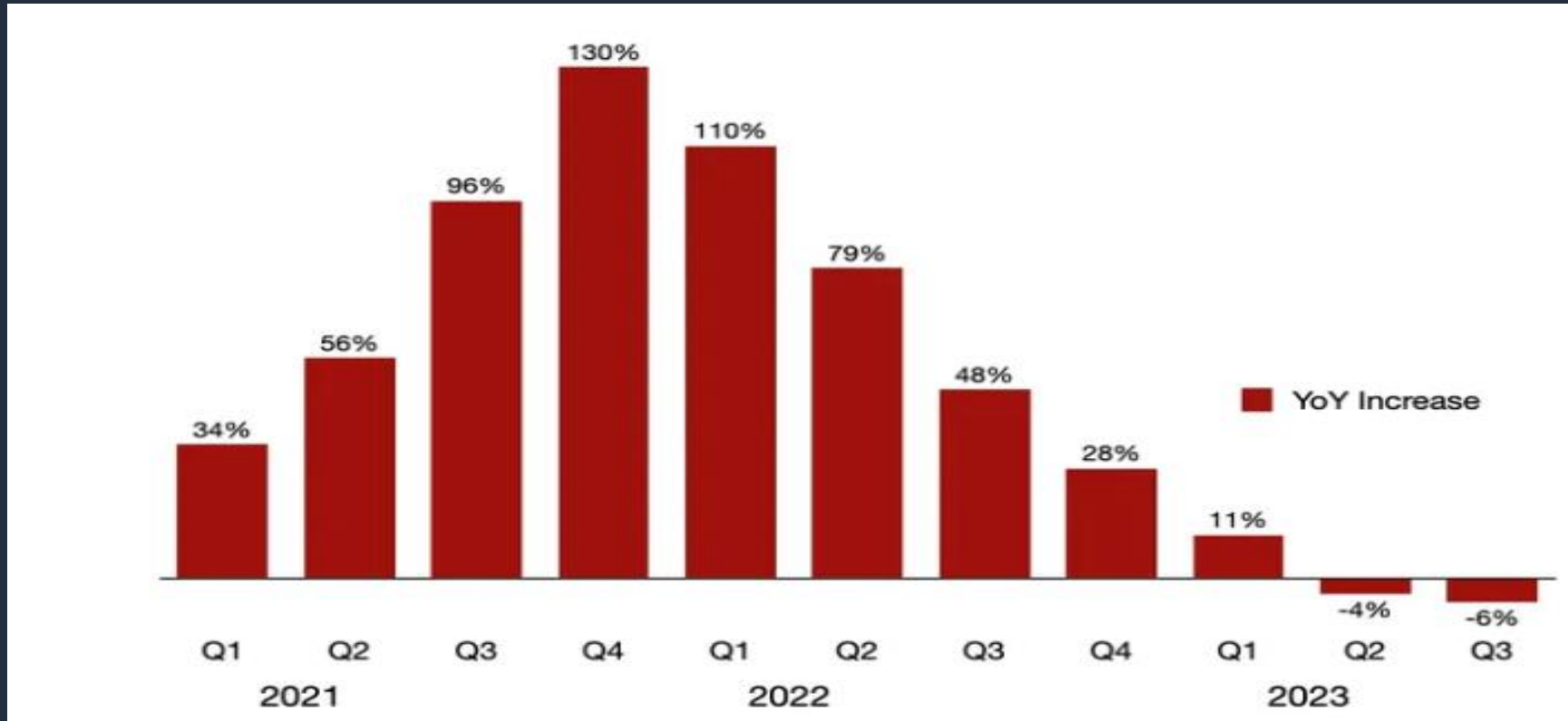


End-of-life systems replaced or protected



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

Cyber Insurance Partners have committed to generating a quote for AWS customers within two business days of the request. 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...



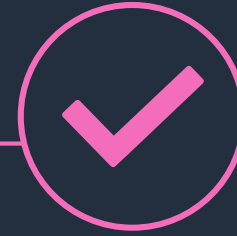
**Allows for
State entities
to procure
security
capabilities
based specific
cyber gaps**



**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



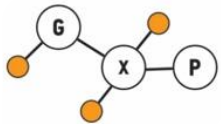
CCCS
PIPEDA



CJIS



FERPA



GxP



MPAA



SEC Rule
17a-4(f)



VPAT
Section 508



FISC



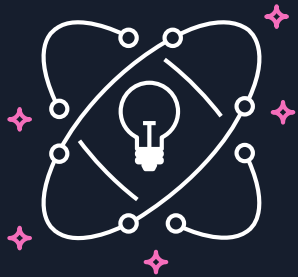
G-Cloud



What about generative AI?

- ✓ Ease of use – Reduce friction to deployment
- ✓ Security and privacy – Top of mind for customers
- ✓ Choice – Multiple models to meet your needs
- ✓ Availability – Scale to meet customers' needs

Generative AI enables innovation and unlocks new business value



CREATIVITY

Create new content and ideas, including conversations, stories, images, videos, and music



PRODUCTIVITY

Radically improve productivity across all lines of business, use cases, and industries



CONNECTIVITY

New ways to connect and engage with customers and across organizations

Security considerations for generative AI

COMPLIANCE & GOVERNANCE

The policies, procedures, and reporting needed to empower the business while minimizing risk

Create generative AI usage guidelines

Establish process for output validation

Develop monitoring and reporting processes

LEGAL & PRIVACY

The specific regulatory, legal, and privacy requirements for using or creating generative AI solutions

Retain control of your data

Encrypt data in transit and at rest

Support regulatory standards

CONTROLS

The implementation of security controls that are used to mitigate risk

Human-in-the-loop

Explainability and audibility

Testing strategy

Identity and access management

RISK MANAGEMENT

Identification of potential threats to generative AI solutions and recommended mitigations

Threat modeling

Third-party risk assessments

Ownership of data, including prompts, and responses

RESILIENCE

How to architect generative AI solutions to maintain availability and meet business SLAs

Data management strategy

Availability

High Availability and Disaster Recovery strategy

KEY CONSIDERATION: TRUST

Responsible AI dimensions

FAIRNESS

Considering impacts on different groups of stakeholders

EXPLAINABILITY

Understanding and evaluating system outputs

CONTROLLABILITY

Having mechanisms to monitor and steer AI system behavior

SAFETY

Preventing harmful system output and misuse

PRIVACY AND SECURITY

Appropriately obtaining, using and protecting data and models

GOVERNANCE

Incorporating best practices into the AI supply chain, including providers and deployers

TRANSPARENCY

Enabling stakeholders to make informed choices about their engagement with an AI system

VERACITY AND ROBUSTNESS

Achieving correct system outputs, even with unexpected or adversarial inputs

Evolving best practices to build generative AI responsibly

- ✔ Define use cases—the more specific and narrow, the better
- ✔ Prioritize education and diversity in your workforce
- ✔ Assess risk with a performance evaluation
- ✔ Test, test, test
- ✔ Continually iterate across the AI lifecycle
- ✔ Introduce governance policies with accountability and measurement

Enterprise-wide security data analysis is challenging



Inconsistent and incomplete data

Logs and alerts in varying formats scattered across the organization in tough to find data silos



Growing volumes of security data

Explosion of security and log data means more time wrangling data than actual analysis



Inefficient use of data across use cases

Need for specialized tools can result in data duplication and reprocessing for each use case

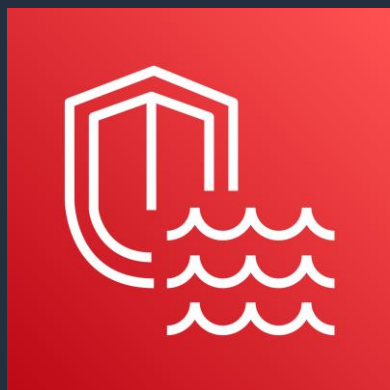


Lack of direct control over processed data

Certain tools store processed data in their own system. This reduces your flexibility in using that data.

Security Lake

AUTOMATICALLY CENTRALIZE SECURITY DATA INTO A PURPOSE-BUILT DATA LAKE IN A FEW CLICKS



Centralize data automatically from cloud, on-premises, and custom security sources across regions

Optimize and manage security data for more efficient storage and query performance

Normalize data to an industry standard to easily share and use with multiple analytics tools

Analyze using your preferred analytics tools while retaining control and ownership of your security data

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”
- ✓ Reassess/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

