Building Resilience and Effective Collective Defense

Maria S Thompson

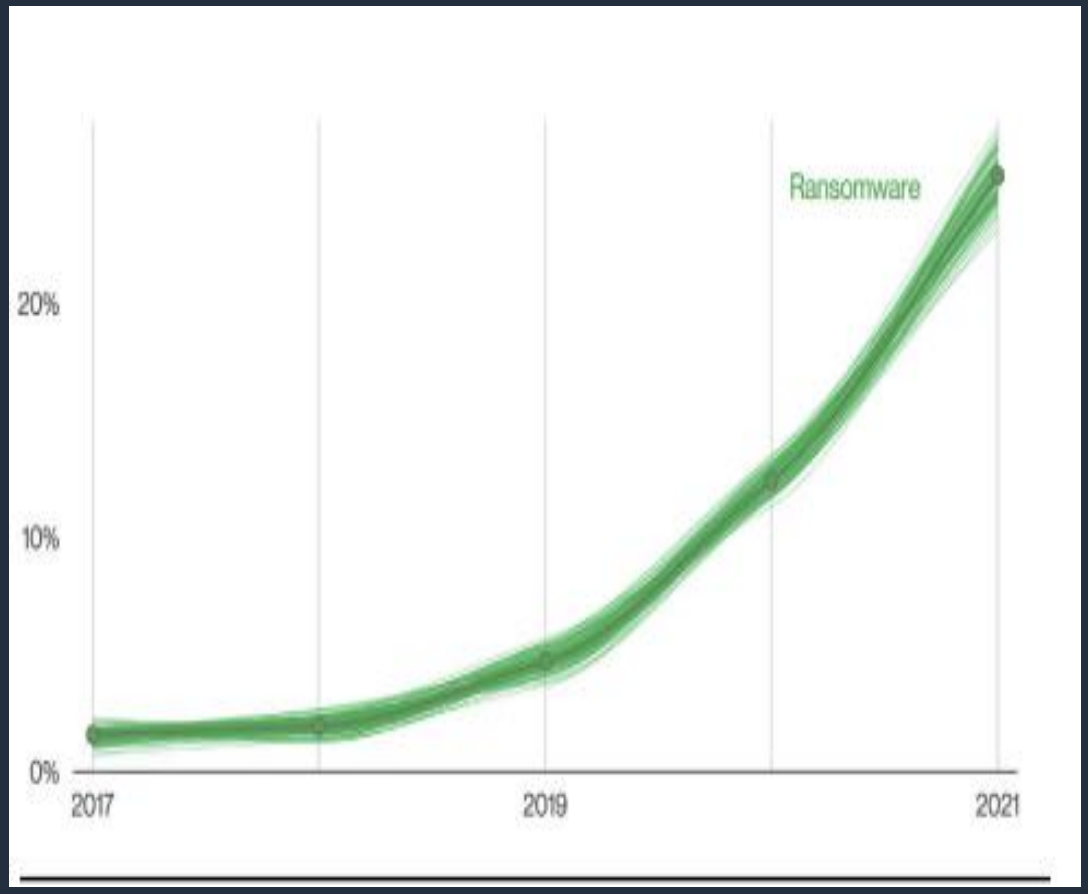
SLG Executive Govt Advisor – Cybersecurity
AWS

AGENDA

- Threats Facing State and Local Government
- Collective Defense & Risk Mitigation Strategies
- Resilience – Why is it important
- Whole of state/government approach to cyber
- State and Local Cybersecurity Grant Program (SLCGP)
- Cyber & Privacy Policy Snapshot
- Opportunities for success

Threats Facing State and Local Government (SLG)

- Supply Chain attacks/Third Party Risks
- Critical Infrastructure attacks
- Business Email Compromises
- Insider Threats
- Ransomware/Phishing attacks
- Emerging Threats – The unknown

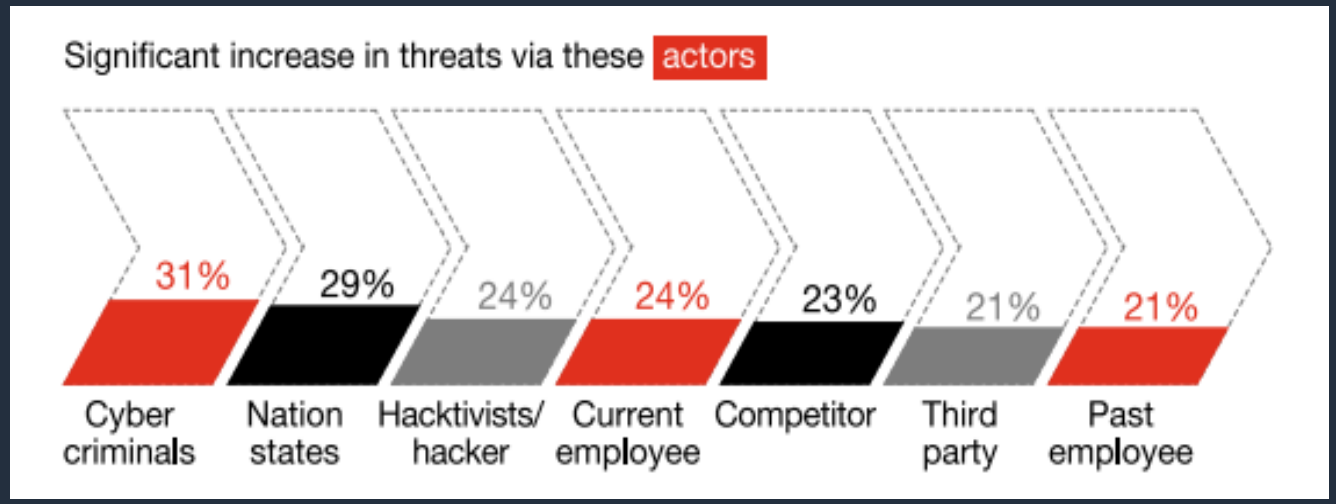


Source: 2022 Verizon Data Breach Investigations Report

Threats Facing State and Local Government (SLG)

2020 Deloitte - NASCIO Cybersecurity Study identified these top barriers for States to overcome:

- Insufficient cyber budget
- Lack of skilled cyber professionals
- Legacy Infrastructure and solutions
- Inadequate availability of cybersecurity professionals
- Lack of recurring/dedicated cyber budget



Source: 2021 PWC – Cyber-ready-Today and for tomorrow

Ransomware is a growing business risk

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

Ransomware

“ransomware has become a scourge on nearly every facet of our lives, and it’s a prime example of the vulnerabilities that are emerging as our digital and our physical infrastructure increasingly converge”

Jen Easterly - Director of DHS CISA

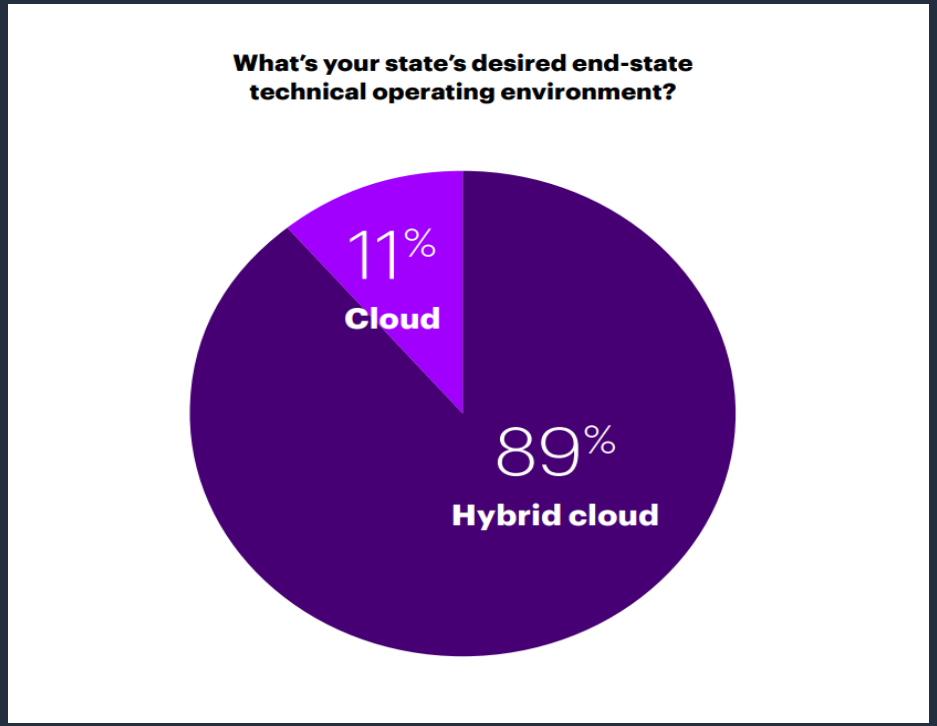

STATE - REGIONAL

South Carolina municipalities facing nonstop cyberattacks, working from home a potential threat


FBI, CISA warn cyberattacks against schools ‘may increase’ as semester begins

Collective Defense & Risk Mitigation Strategies

- Take a data centric approach to cyber
- Take part in collective defense opportunities
- Prioritize mission critical systems/data
- Use integration/orchestration for efficiency
- Build resiliency into infrastructure and processes
- Redefine what success looks like:
  - χ **OLD**: We never do down
  - ✓ **NEW**: Recover with CIA in Minutes



2021 NASCIO & Accenture Cloud Study

Why Start With Recovery & Resilience?

- Recovering your applications and data means you don't have to pay a ransom or reduce the impact of natural disaster occurrence
- No way to prevent accidental / incidental outages so prepare now to avoid downtime
- Automated point-in-time recovery allows you to rollback to a moment before the incident
- Quick to implement with the ability to test failover without impact
- Gain additional resilience by adding immutable backups

"Ransomware is a symptom of a lack of resilience…"

Whole of State / Government Cyber Approach

Methods

- Endpoint Protection
- Shared Service Agreements
- Incident Response & Forensics
- Network monitoring
- Cyber Awareness & Training
- Phishing simulations
- Mobile App security
- Policy development
- Security Assessments

Benefits

- ✓ Unified enterprise driven model
- ✓ Leverages volume discount opportunities
- ✓ Builds trust and enables information sharing
- ✓ Educates state leaders on gaps within the state
- ✓ Supports sound decisions and prioritized actions
- ✓ Simplifies and standardizes security architecture
- ✓ Reduces stress on resources

State and Local Cybersecurity Grant Program (SLCGP)

The goal of SLCGP is to assist SLT governments with managing and reducing systemic cyber risk.

- Objective 1: Develop and establish appropriate governance structures, including developing, implementing, or revising cybersecurity plans, to improve capabilities to respond to cybersecurity incidents and ensure continuity of operations.

- Objective 2: Understand their current cybersecurity posture and areas for improvement
- based on continuous testing, evaluation, and structured assessments.

- Objective 3: Implement security protections commensurate with risk.

- Objective 4: Ensure organization personnel are appropriately **trained** in cybersecurity, commensurate with responsibility

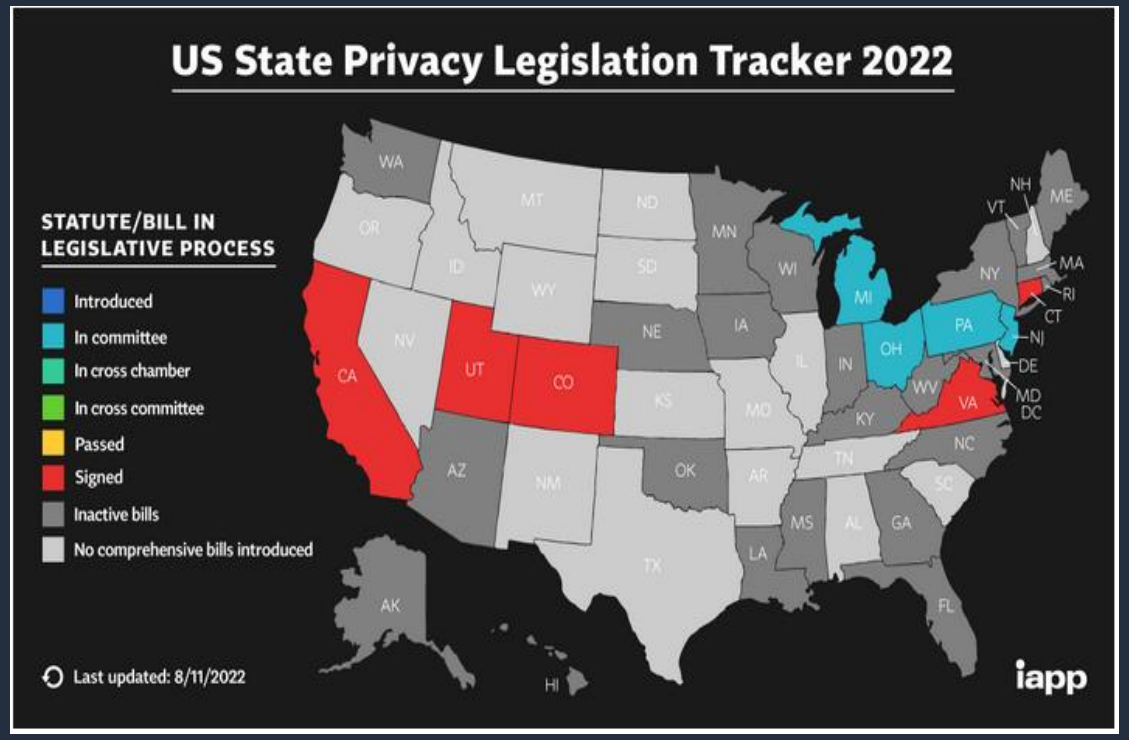
****South Carolina is eligible for $3,661,568**

Security legislation

- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA)
- 24 states enacted 41 bills in 2022
- 12 states address ransomware with varying success
- 23 states address phishing scams
- 26 states address denial of service
- 30 states have statewide cybersecurity task forces

Privacy laws

- The collection, use, and sharing of customer data is under increasing public scrutiny.
- Governments are enacting data protection laws, like the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA)
- 32 States have Consumer Privacy legislation, inactive/active bills



Opportunities for Success

- ✓ Develop a continuous monitoring plan
- ✓ TEST, TEST and…TEST
- ✓ Prioritize data resilience
- ✓ Leverage cloud for resiliency, security and immutable backup capabilities
- ✓ Implement information sharing for collective defense
- ✓ Modernize aging infrastructure
- ✓ Re-assess/review security architecture periodically
- ✓ Use integrated solutions w/automation
- ✓ Leverage federal funding opportunities

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

THANK YOU!

“Invest in progress, NOT maintenance”

Maria Thompson
thammari@amazon.com