WHITE PAPER

Beyond traditional boundaries: A blueprint for Whole-of-State cybersecurity

This white paper aims to provide guidance on how to develop a Whole-of State cybersecurity strategy that is based on best practices develop in real-world implementation. It will bring together the key components of an evidence-based cybersecurity strategy, including the State and Local Cybersecurity Grant Program funding and provide practical guidance on how to implement these strategies and measure their effectiveness.

LUMEN®
The Platform for Amazing Things℠

State and local governments continue to face demand for scalable and connected citizen services. Yet, as digital infrastructure is modernized, the potential cybersecurity attack surface widens, opening the door to new attacks that threaten to disrupt government operations. Each incident has tangible and intangible impacts on the government's ability to deliver support and protection for its citizens.

Compounding this challenge is the growing talent shortage and typically siloed approach to managing cybersecurity risks. As each jurisdiction and agency attempts to secure their own digital borders, cybersecurity threats often hinder interoperability, data sharing, and effective operations. The weakest entity can easily be targeted and could affect the entire State.

To combat the escalating threat of cybersecurity attacks, the Department of Homeland Security announced the State and Local Cybersecurity Grant Program (SLCGP), which will provide one billion dollars to be awarded over four years. This presents an unprecedented opportunity for all levels of state government to come together to fight a common problem—escalating cyber threats—through an equitable process that leaves no agency behind.

SLCGP funding will be awarded to each state, with specific requirements to allocate the funding across jurisdictions throughout counties, municipalities, and tribal territories. This level of coordination within all levels of state government requires a coordinated cybersecurity strategy and support of multiple stakeholders in participating jurisdictions.

About Lumen

For over a half a century, Lumen has helped public agencies accelerate transformation and enable progress to keep America safer, healthier, engaged and ready for what's next. Lumen enables government business and empowers public servants through collaboration, standardized governance, common tooling, resource optimization, and automation. All of this is delivered by Lumen with a focus on sustainable and equitable growth in line with Lumen's core values of Teamwork, Trust & Transparency.

> Everything in a state is connected. Local communities are connected to the state government and each other. To protect any one piece of IT infrastructure in the state, you have to protect it all,"

— Vinod Brahmapuram
Senior Director of Security at Lumen
and former CISO for Washington State

Bringing together people, processes and policies to achieve cybersecurity governance

Implementing a Whole-of-State cybersecurity strategy begins with creating a truly collaborative governance process that develops trust and a shared vision between participants from all levels of government. According to Brahmapuram,

> We are seeing misconceptions where people think this is a 'Big Brother' trying to reach in and take over. That's not really what this is; this is about putting together a team."

Trust will improve communication between state and local governments to understand risks and share information so they can respond to cyber incidents effectively.

In the context of cybersecurity, collaborative governance can help state and local governments leverage the expertise, resources, and capabilities of different stakeholders to improve their cybersecurity posture and respond to cyber threats.

One example of collaborative governance in cybersecurity is the Multi-State Information Sharing and Analysis Center (MS-ISAC), which is a partnership between the Center for Internet Security and state, local, territorial, and tribal governments. The MS-ISAC provides a range of cybersecurity services and resources to its members, including threat intelligence sharing, incident response support, and cybersecurity training and awareness programs.

By creating information sharing and analysis centers (ISACs) across state and local levels, it creates a more coordinated and agile response when an incident occurs.

Blueprint to prioritize collaborative governance

- Establish and build trusted relationships with diverse stakeholders, including government agencies, private sector organizations, and civil society groups.
- Develop information sharing and analysis centers at the state and local level to facilitate deeper collaboration.
- Building in cybersecurity policies and regulations that promote collaboration and information sharing among the different stakeholders.

The Lumen advantage

Lumen's dedicated team includes professionals with decades of experience as state and local CISO's and IT leadership who understand the importance of collaborative governance:

- We assist with developing governance programs that align with existing operations and goals.
- We provide the insight, data, and metrics needed for successful planning.

Measure progress with ongoing assessments and evaluations

In a Whole-of-State cybersecurity effort, each jurisdiction must commit to conduct ongoing assessments and evaluations, monitor timely and accurate data, and practice holistic cybersecurity hygiene to prevent attacks when possible, and remediate them quickly before the attackers have time to seize full control.

Since the pandemic, the rise in ransomware and cyberattacks have dispruted operations across jurisdictions including transportation, judicial systems, public safety, public health systems and more. Several of these attacks demonstrated the severity of dwell time, which is the time between the identification of a malicious actor and when the attack is mitigated. The longer an attack is uncontained, the more opportunity to cause damage, interrupt operations, and spread harmful tactics across the state, affecting jurisdictions, supply chain, and citizens. These gaps are often most apparent with small municipalities that don't have the resources to assess their security posture.

To minimize risk, it is critical to understand a state and its jurisdictions' current cybersecurity capabilities and maturity down to its smallest entities. Ongoing assessment and rigorous evaluation of threat vectors, capabilities, and unique business risks is critical and requires sharing relevant data with the state-wide team.

Center for Internet Security Controls for essential cyber hygiene

1. Inventory and control of enterprise assets
2. Inventory and control of software assets
3. Data protection
4. Secure configuration of enterprise assets and software
5. Account management
6. Access control management
7. Continuous vulnerability management
8. Audit log mangement
9. Email and web browser protections

Blueprint to prioritize effective cybersecurity assessment

1. **Regularity:** Assess and evaluate on a consistent basis to identify vulnerabilities, measure risks, and establish a baseline for measuring progress.
2. **Comprehensive approach:** Assess both technical and non-technical elements to factor in human and organizational impact. Not only technical systems and process but also human and organizational factors that impact cybersecurity.
3. **Use of standards and frameworks:** Leverage existing resources, such as the NIST Cybersecurity Framework, to guide the assessment process.
4. **Involvement of all stakeholders:** Include multiple perspectives across the organization - management, IT staff, and end-users - in the process.
5. **Documentation:** Create reports that identify vulnerabiilties and gaps. Use this documentation to mesure progress over time.
6. **Risk prioritization:** Assign risk scoring based on impact to an organization's operations and risk appetite.
7. **Follow-up action:** Create a plan to address prioritized risks and vulnerabilities and continue to monitor to ensure corrective measures are effective.

The Lumen advantage

Lumen delivers a blend of managed security solutions combined with professional security services and proven cybersecurity technologies to:

- Assist with identifying cybersecurity risks to systems, assets, data, and organizational policies within and across jurisdictions.
- Implement cybersecurity assessments and continuous monitoring to develop a common framework across the jurisdiction's systems, applications, data, and users.

Remediation and mitigation

Attacks will occur at all levels of the state-wide partnership before, during, and long after the Whole-of State effort is developed. At the time of an incident, the state's cyber task force must quickly identify the nature of the incident and have a tested, proven method of sharing information that enables each jurisdiction to act immediately to remediate and mitigate the impact of the attack. James Weaver, Secretary and Chief Information Officer for the North Carolina Department of Information Technology, explains,

> "The joint cyber task force is not there to run day-to-day operations, it's there to resolve the incident, contain it, eradicate it."

— James Weaver
Secretary and Chief Information Officer for the North Carolina Department of Information Technology

In the wake of numerous high-profile breaches across state and local government agencies, a South-Atlantic state needed a full security program review to adapt to the rapidly changing threat landscape. The jurisdiction had a highly complex and dispersed environment, with disparate security technologies in place. Leadership recognized that their workforce of skilled cyber experts was not large enough to maintain the round-the-clock coverage required.

1. "How to Drive a Whole-of State Cyber Strategy," GovLoop.

Lumen partnered with the State to provide:

1. Staffing, which included a dedicated team to support a fully managed security service, including 24/7 security monitoring, incident response, and firewall management.

2. Development and implementation of a 5-to-7-year plan for technology refresh involving their entire security infrastructure.

3. Establishment of reliable and auditable security controls for its agencies' IT systems and data, while providing thought leadership and strategy development services to help mature its security posture.

The Lumen advantage

Lumen provides managed security services to help organizations monitor their network and detect potential threats in real-time.

- Protect against cyberattacks that flood the network, making it unavailable to legitimate users.
- Implement identity access management, threat detection and response, compliance reporting.
- Emergency response to incidents with forensics analysis, containment and recovery.

Blueprint to prioritize remediation and mitigation

1. Reduce the dwell time attackers have to seize control. Immediately isolate and contain the affected systems to prevent further damage or data loss.

2. Document the incident completely, including the steps taken during the incident response process.

3. Develop and maintain a comprehensive and well-tested incident response plan. The plan should outline procedures for responding to cyber incidents and provide clear guidance on how to contain, remediate, and recover from an incident.

4. Maintain accurate and up-to-date asset inventories to identify potential vulnerabilities and ensure that all systems are patched and updated in a timely manner.

5. Implement strong authentication mechanisms, such as multi-factor authentication, to protect against unauthorized access to systems and data.

Overcoming the shortage of cybersecurity experts in the workforce

> "One of the biggest challenges we face as an industry is the shortage of qualified cybersecurity professionals. This shortage is particularly acute at the state and local government level, where budgets are limited and competition for talent is intense."

—MS-ISAC Cybersecurity Primer for State and Local Governments (March 2021)

According to the 2022 Deloitte-NASCIO Cybersecurity Study, 52 percent of the respondents said that inadequate availability of cybersecurity professionals was a barrier to addressing cybersecurity challenges. This is a shortage that can leave critical gaps in every jurisdiction's IT workforce especially, smaller and rural communities.

Without the proper resources, staffing, and training, the smallest communities become the most vulnerable for attack, even with the appropriate assessments and evaluation and the technology solutions in place. Additionally, for the staff managing security operations, they often face burnout, and the cyber "fog of war" where they cannot keep up with the number of alerts and alarms coming from various security devices nor enforce security policies and practices.

For example, **a large county in the Mid-Atlantic region** wanted a modernized, simplified, and upscaled environment, along with a scalable SIEM environment and proactive views into specific and varied KPIs. To meet the customer's needs, Lumen leveraged our network infrastructure capabilities, layered with managed and professional services, and our strong ecosystem of partners to provide:

- Modernized and upgraded the state's backbone environment and offered a fully managed statewide network including ethernet, WAVEs, IP and cloud connectivity;
- Simplified managed firewall services;
- Managed and implemented a scalable Security Information Event Management (SIEM) systems and other security services;
- Managed threat detection and response.

Identifying the right partners that can alleviate the resource burden while offering a holistic approach that leaves no agency or jurisdiction behind, is critical to the success of a Whole-of-State security strategy.

Blueprint to prioritize managed security

1. Assess relevant skills and availability across the existing IT workforce, and identify gaps.
2. Identify partners or resources that can ease the burden of 24/7 monitoring, remediation, and mitigation.
3. Implement cybersecurity excercises and skills training programs to enhance internal staff capabilities.
4. Identify a partner to provide the latest threat and cyber intelligence data with rapid defense capabilities.

The Lumen advantage

Lumen can alleviate cybersecurity burnout and bolster resources with:

- Managed security operations for threat detection, rapid threat response and continuous montioring.
- Cybersecurity training to help workforce develop the skills needed to combat threats.
- Unique threat intelligence data and reporting to help your staff prioritize.

Conclusion

With the upcoming opportunity to secure SLCGP funding for your state, Lumen encourages State legislators and State IT leaders to take a holistic approach to its cybersecurity strategy and work with a partner that can support a centralized Whole-of-State security approach to ensure collaboration across every jurisdiction.

The Lumen advantage

Lumen connects the world. We are dedicated to furthering human progress through technology by connecting people, data, and applications – quickly, securely, and effortlessly. Lumen combines government expertise and trusted technology to deliver next-gen citizen experiences. With an adaptive network, cloud-based services, and built-in security, Lumen's platform can help state leaders improve the security of critical infrastructure and resilience of the services that state, local, and territorial governments provide to their communities.

LEARN MORE

888-597-2455 | lumen.com | info@lumen.com

Services not available everywhere. Business customers only. Lumen may change, cancel or substitute products and services, or vary them by service area at its sole discretion without notice. ©2023 Lumen Technologies. All Rights Reserved.

LUMEN®