rubrik

WHITE PAPER

THE WHOLE OF STATE APPROACH:

SAFEGUARDING OUR DIGITAL COMMUNITIES

INTRODUCTION

THE STATE OF STATE, LOCAL, AND TRIBAL GOVERNMENTS: PROTECTING ASSETS IN AN INCREASINGLY DIGITAL WORLD

The “Whole of State” initiative emerged as local governments faced increasing cyberattacks and lacked the resources to defend themselves, prompting state governments to intervene. This approach was further solidified by the State and Local Cybersecurity Grant Program (SLCGP), which mandated states to take on a more active role in cybersecurity.

Under this approach, states can offer a wide range of services to meet the diverse needs of State, Local, Tribal, and Territorial (SLTT) government agencies. This includes anti-phishing, security awareness training, advanced endpoint protection, converged endpoint management, multi-factor authentication, web application firewalls, incident response planning, vulnerability management, data encryption, network segmentation, and identity and access management.

This paper will examine the Whole of State approach, which emphasizes the importance of shared relationships and trust, recognizing that cybersecurity is only as strong as its weakest link. Then, we’ll take a look at how fostering these connections can help organizations better defend against escalating cyber threats and address resource constraints and vulnerabilities within state and

THE STRATEGY FOR WHOLE OF STATE CYBERSECURITY

WHAT IS WHOLE OF STATE CYBERSECURITY?

The Whole of State cybersecurity strategy fosters a cooperative environment where leaders collaborate to share or pool resources, exchange information, and potentially utilize federal and state funding to combat shared cyber threats. The goal of this approach is to create a unified front against cyber threats, helping agencies to realize economies of scale, standardize capabilities, and share training and best practices.

The groundwork for Whole of State collaboration began with the widespread deployment of Internet broadband access over the past 20 to 30 years, extending beyond population centers and connecting local governments with dark fiber. This infrastructure is crucial for enabling collaboration, especially in states that have invested heavily in broadband. Additionally, the SLCGP, established under the 2021 Infrastructure Investment and Jobs Act, allocated approximately $1 billion over four years (2022-2025) to enhance the cybersecurity posture of SLTT governments across the U.S.

The central idea driving the Whole of State approach is that we are all better together and if we pool our resources and knowledge, we can yield better outcomes than any single organization could deliver on its own. This includes taking federal and state-level funds, as well as engaging with local stakeholders, whether that be local governments, county governments, city governments, or schools to address cybersecurity risks and threats to SLTT systems.

KEY COMPONENTS OF WHOLE OF STATE CYBERSECURITY

Information Sharing and Collaboration

Resource Sharing: States pool their resources to enhance their collective cybersecurity posture. This includes sharing threat intelligence, best practices, and technological tools. This is a very common practice in the U.S. military, which deploys joint task forces from all the services to solve urgent and/or specialized problems.

Interagency Cooperation: Collaboration between state agencies, local governments, and tribal entities ensures a coordinated response to cyber incidents. Regular meetings and communication channels are established to facilitate this cooperation.

Economies of Scale: Joint procurement and more thorough evaluations, as well as shared services, can reduce costs and eliminate duplication of efforts.

Employee Training and Awareness

Continuous Training Programs: Regular training sessions for employees at all levels ensure that they are aware of the latest cyber threats and best practices for mitigating them. This includes phishing simulations, cybersecurity workshops, and certification programs.

Awareness Campaigns: Public awareness campaigns help educate citizens about cybersecurity risks and promote safe online behaviors. These campaigns can be conducted through various media channels and community outreach programs.

Federal and State Funding Utilization

Grants and Financial Support: States can access federal grants and funding programs, such as the SLCGP, aimed at improving cybersecurity infrastructure and capabilities. This financial support is crucial for implementing advanced security measures and technologies. States often allocate state budget funds to support the local governments and cover the SLCGP cost share.

Public-Private Partnerships: Engaging with private sector partners can provide additional resources and expertise. These partnerships can help bridge gaps in capabilities and offer innovative solutions to emerging threats.

Threat Monitoring and Incident Response

Advanced Threat Detection: Implementing sophisticated threat detection systems allows for the early identification of potential cyber threats. This includes using artificial intelligence (AI) and machine learning (ML) to analyze network traffic and detect anomalies.

Incident Response Teams: Dedicated teams are established to respond to cyber incidents promptly. These teams are trained to handle various types of cyber threats and work to minimize the impact of attacks on state and local systems. A comprehensive incident response plan must include a sound recovery strategy, which is all about returning to normal operations after a threat has been eliminated.

STATES LEADING THE WAY

Arizona: Arizona has developed a comprehensive cybersecurity framework that includes a centralized security operations center (SOC) and a robust incident response plan. Arizona's statewide cyber readiness program provides resources to local and tribal government entities, including anti-phishing, security awareness training, advanced endpoint protection, converged endpoint management, multi-factor authentication, and web application firewall. The state also emphasizes public-private partnerships to enhance its cybersecurity capabilities.

Indiana: Indiana's cybersecurity strategy focuses on workforce development and education. The state has established cybersecurity degree programs and training initiatives to build a skilled workforce capable of addressing modern cyber threats.

North Carolina: North Carolina has implemented a statewide cybersecurity task force that coordinates efforts across different agencies and local governments. The state also invests in advanced threat detection technologies and continuous monitoring systems.

New York: New York's approach includes extensive collaboration with federal agencies and neighboring states. The state conducts regular cybersecurity exercises and drills to test its preparedness and improve its response capabilities.

STRENGTHENING CYBER DEFENSES

WHY CYBER RESILIENCE IS THE KEY

Adopting a Whole of State approach requires a phased strategy: crawl, walk, run. There is no one technological silver bullet. Cyber resilience has become a critical component for organizations aiming to safeguard their data and maintain operational continuity. It encompasses a range of strategies designed to protect, detect, respond to, and recover from cyber threats.

THE NEED FOR BACKUP

A critical first step for governments is to focus on hardening backups. Air gapping and data immutability can protect data from the onset of an attack. Modernizing and simplifying backup environments is crucial, as complexity often leads to vulnerabilities and lengthy downtime. However, hardening backups is just the beginning. The following points highlight key aspects of cyber resilience, including hardening backups, modernizing backup environments, and implementing comprehensive cyber recovery measures.

1 Hardening Backups

Air Gapping: This involves creating a physical or logical separation between the backup data and the network, reducing accessibility to attackers. By storing backups on devices not connected to the internet or main network, air gapping ensures that even if the primary network is compromised, the backup data remains secure.

Logical Air Gapping: A logical air gap refers to the segregation and protection of a network-connected digital asset by means of logical processes. For example, through encryption and hashing, coupled with role-based access controls, it is possible to achieve the same security outcomes that are available through a physical air gap. Even if someone can access the digital asset, the asset cannot be understood, stolen, or modified.

Data Immutability: Immutability ensures that once data is written, it cannot be altered or deleted, protecting it from ransomware and other malicious activities.

2 Modernizing Backup Environments

Simplifying and modernizing backup environments reduces complexity, which is often a source of vulnerabilities. This modernization includes adopting cloud-based solutions and integrating advanced security features.

3 Comprehensive Cyber Recovery

Rapid Recovery: In the event of a cyber incident, the ability to quickly restore data and systems is crucial. This minimizes downtime and reduces the impact on constituents.

Data Visibility and Classification: Gaining comprehensive visibility into where sensitive data lives and who has access to it is crucial to reducing data exposure and exfiltration risks.

Data Integrity: Ensuring that the recovered data is accurate and uncorrupted is essential for maintaining trust and operational continuity.

Impact Assessment: Identifying which data has been impacted by the attack helps in prioritizing recovery efforts.

4 Cyber Resilience

Proactive Measures: Implementing proactive measures such as regular testing of backup and recovery processes, continuous monitoring, and threat intelligence integration is integral to maintaining a secure cyber posture.

Incident Response Planning: Developing and regularly updating incident response plans ensures preparedness for various types of cyber incidents.

THE ROLE OF RUBRIK IN A WHOLE OF STATE MODEL

Rubrik offers a comprehensive data management and protection solution that can significantly enhance the cybersecurity posture of SLTT government agencies within a Whole of State model. Rubrik can help with the operationalization of the U.S. National Institute of Standards and Technology (NIST) Cybersecurity Framework 2.0, particularly for controls that deal with identifying data assets, protecting data, offering immutable backups and encryption, and detecting threats and assessing their impact, and recovering from cyber threats.

Here are some key Rubrik benefits:

Unified Data Protection: Rubrik provides a single platform for managing data backup and recovery across various environments, including on-premises, cloud, and hybrid setups. This unification simplifies and ensures consistent protection policies across all agencies.

Automated Backup and Recovery: Automated backup and recovery capabilities ensure that critical data is regularly backed up and can be quickly restored in the event of a cyber incident. This automation reduces the risk of human error and ensures data availability.

Immutable Backups: Rubrik creates immutable backups that cannot be altered or deleted by ransomware or other malicious actors. This immutability ensures that backup data remains secure and can be relied upon for recovery.

Testing Backups: Testing backups is critical to ensure that data can be restored when needed. Rubrik ensures backup reliability through automated validation, which includes end-to-end tests and application checks. Administrators can verify backups using the Rubrik REST API to ensure data integrity. Additionally, Rubrik offers tools for simulating and validating cyber recovery plans in isolated environments, ensuring recovery of service level agreements are met without impacting production.

Scalability: A scalable architecture allows SLTT agencies to easily expand their data protection capabilities as their needs grow. SLTTs require scalable solutions for data management and analytics to handle increasing volumes of data, improve data governance, and leverage data for decision-making and cybersecurity measures as the volume of data and digital services grows. Agencies also need scalable IT infrastructure to support the increasing demands for digital services, cloud computing, and remote work capabilities.

Compliance and Reporting: Robust compliance and reporting features help agencies meet regulatory requirements and demonstrate adherence to cybersecurity standards. This capability is essential for maintaining transparency and accountability.

Enhanced Security: Rubrik integrates advanced security features, such as encryption, role-based access control, and multi-factor authentication to protect data from unauthorized access and breaches.

Simplified Management: With Rubrik's intuitive interface and centralized management, IT teams can efficiently oversee data protection activities across multiple agencies.

Cyber recovery is fundamentally different from recovering from cyber attacks and physical disasters like fires or floods. It requires a specialized approach that includes robust backup strategies, rapid recovery capabilities, and a focus on maintaining data integrity and resilience. By adopting a Whole of State approach and leveraging platforms like Rubrik Security Cloud-Government, government agencies can enhance their cyber resilience and ensure continuity of services in the face of cyber threats.

Learn more about
Rubrik Security Cloud-Government

Read the whitepaper:
Rubrik Security Cloud: The Trusted Data Security Solution for Cyber Recovery

rubrik

Global HQ
3495 Deer Creek Road
Palo Alto, CA 94304
United States

1-844-4RUBRIK
inquiries@rubrik.com
www.rubrik.com

wp-whole-of-state-approach / 20241016