WHITE PAPER

State and Local Governments Take a Risk-based Approach to Cybersecurity

Cybersecurity is no longer an issue that concerns only information technology and security professionals. The risks have become so significant and the impact so strategic that state and local government leaders must consider security within the framework of vital governing priorities. Threats and threat actors continue to increase in volume, and in methods to avoid detection. With private citizen data at risk, the U.S. and Canadian federal governments have placed emphasis on strong cybersecurity policies and implementation. Similar efforts are underway for state and local governments, although the level of cyber protection and maturity varies more widely by locality and department.

The risks apply to many facets of state and local government, including financial systems, citizen portals, benefits and program administration, law enforcement agencies and the national network of fusion centers that are mostly funded and operated through the states. Hacktivists and other politically motivated actors could target any of these systems to steal or expose personally identifiable information, protected health information or criminal justice information, or deface your websites. With such a wide base to cover, governors, mayors and other high-ranking officials should be aware of cyber risks and their potential impacts, and encouraged to champion the cause of cybersecurity from strategic planning, to budgeting, to implementation.

Budget constraints for IT and security initiatives may be higher at the state and local level than for the federal government. The same is true for trained IT security experts, which are harder to find and keep at state and local posts. At the same time, state and local government systems are becoming more interconnected, are migrating to the cloud and are therefore susceptible to more threats and vulnerabilities as a result.

What You Will Learn

- Why a risk-based approach is more strategic than addressing threats
- The importance of continuous monitoring for third-party and cloud security
- The value of information sharing for stronger protection

Who Should Read This White Paper

» Information Security Manager/ Chief Security Officer

» Deputy Secretary/Commissioner

» Directors of Security/IT

There is much the federal government can do to support state and local efforts to improve cybersecurity. Improved coordination and working relationships between federal and state and local counterparts is one way. Increased funding would be another, along with sharing trained security resources to help expand security operations and implement best practices across state and local government agencies. In the meantime, there are several considerations that will help strengthen security posture at the state and local levels, including:

- Assessing risk to apply more strategic protection.
- Using the NIST framework as an effective model for risk-based protection.
- Validating the security of third parties and cloud providers.
- Continuing to emphasize information sharing.

Assessing Risk for Strategic Protection

We now know that cyber risks can never be completely eliminated. This realization requires a shift from prevention-oriented security controls to a risk-based approach that focuses protection, prevention and detection around your organization's most valuable assets in context with the most relevant threats.

This approach will not be as effective in the immediate wake of a breach. Instead, it urges state and local leadership to proactively realign security strategy—driving security technologies, processes and policies in accordance with the areas of greatest risk. State, local, tribal and territorial leadership cannot afford to see security as merely a technical issue to be solved with a purely technical solution. This approach has already been tried and has left state and local governments with a glut of security point products that will not remain effective if left in siloes of protection.

An effective security program should account for people, processes and technology within the backdrop of broader risk management. Rather than being an IT issue, information security should be championed at high levels of state and local government oversight. In addition to strategic risk assessment, state and local governments need a sound approach and technology resources to perform threat detection and incident response—with high levels of visibility and control across the security landscape.

Improving Readiness with Proactive Incident Response

If you try to address every conceivable threat, your team will quickly become overwhelmed with too much information and may be unable to act in the event of a breach. Realistically, you know that it's a matter of when, not if, a security breach will occur. Many state and local governments struggle with incident preparedness. As a result, they face longer, more complicated and more expensive response and remediation to attacks.

Mapping threats to assets and vulnerabilities can help identify potential security risks. Each threat can be associated with a specific vulnerability or even multiple vulnerabilities. Unless a threat exploits a vulnerability, it is not a risk to an asset. Determining the combinations that apply to each agency and government network can help reveal the impact and likelihood of security breaches.

Then you can build a flexible plan designed to respond quickly and effectively to any incident. You can align policies, procedures and controls against targeted threats, and evaluate the methods used to secure normal and privileged users.

An effective incident response plan starts by defining the set of priorities that will govern response activities based on the specialized needs of the agency. Next, the plan should create generic action plans for common incident situations that define high-level procedures for response and recovery related to those priorities. To avoid delays and confusion during an incident, the plan also needs to define roles and responsibilities, and empower resources to act accordingly with the proper permissions.

With strategic risk assessment, incident response planning and access to the latest security intelligence on threat actors and their tradecraft, state and local governments can better understand their exposure to targeted threats. They can also enhance preparedness to address even sophisticated and evasive advanced persistent threats (APTs).

State and local governments want to respond, not react, to threats. Incident response planning can invigorate the agency's response time, helping to minimize the impact, duration and cost of a breach. The importance of properly managing a security incident is also emphasized in the NIST framework, a helpful resource for achieving the right mix of resources, processes and technology for stronger protection and reduced risk.

Using the NIST Framework as an Effective Model for Risk-Based Protection

President Obama's 2013 Executive Order on improving cybersecurity resulted in the National Institute of Standards and Technology (NIST) Cybersecurity Framework. Since then, companies and government agencies have been working to implement the voluntary standards contained in the framework for improved agnostic security practices. NIST also created a common language and baseline for organizations to discuss and review security intelligence and response capabilities.

Even though NIST was originally created to focus on U.S. critical infrastructure providers, its risk-based security model can help state and local governments assess their risk, and improve security guidelines and practices accordingly. In fact, it is being adopted by public and private entities around the world. Improved security communications, increased collaboration across departments and agencies and streamlined regulatory compliance are all ancillary benefits of implementing the NIST framework.

When state and local entities have to fight for every budget dollar, they will seek to quantify security spending around documented proof of a pain point or problem area. The framework can help guide security spending where generally accepted accounting procedures for baseline security do not exist. Over time, the standard will give state and local governments a helpful touchstone by which to measure security performance and the effectiveness of security spending and resource allocation.

Validating Security with Continuous Monitoring

As part of a risk-based approach to cybersecurity, state and local governments must consider the risks to data shared with partners, other agencies and third parties, as well as the risks introduced by digital government initiatives. Cloud-based payments systems, portals and other e-Government initiatives designed to serve citizens must be properly secured from threats. Even if traditional government systems are locked down, insecure connections with third parties, cloud platforms and other agencies can unravel the strongest protection strategies.

Before the cloud, state and local government employees may have only used vetted computer equipment and software, and agencies maintained their own private data centers. Now, state and local government employees are using public cloud computing, and the stakes for protecting private citizens' data like student records and driver's license numbers are extremely high. A hybrid IT environment means more management consoles, and that means more challenges with regard to visibility, integration and Federal Information Security Management Act (FISMA) compliance.

The NIST Cybersecurity Framework

The NIST Cybersecurity Framework is voluntary guidance based on existing standards, guidelines and practices for critical infrastructure organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it can foster risk and cybersecurity management communications amongst both internal and external organizational stakeholders.[1]

[1]NIST Cybersecurity Framework Frequently Asked Questions; https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics#framework

While cloud computing offers major efficiency and cost savings for state and local governments, agencies that want to take full advantage of hybrid IT will need global security visibility across cloud, on-premises and customer premises equipment (CPE) environments.

FISMA, Federal Information Processing Standards (FIPS) requirements and the NIST framework address the security controls and monitoring you have in place. To achieve FISMA compliance, your government institution will need strong monitoring and management capabilities, including:

- Management and monitoring of Intrusion Detection and Prevention Systems (IDS/IPS), firewalls and gateway appliances.
- 24x7 security monitoring of logs and alerts by security professionals.
- Comprehensive log management including forensically-sound log retention.
- On-demand security information management with compliance reporting.
- Vulnerability scanning for the network perimeter, internal systems, web and cloud applications.
- Threat intelligence with early warnings for the latest attacks, vulnerabilities and trends.

With superior monitoring and visibility across the entire security landscape, you will gain greater efficiency in security operations and enhanced protection. Threat intelligence aligns closely with security monitoring to improve state and local government's security posture.

The Value of Information Sharing for Stronger Protection

Cyber threats are rapidly evolving, and information sharing between public, private, federal, state and local entities provides vital security intelligence to combat the wide array of malicious cybercriminals. At the same time, these agencies can have vastly different structures, technical connectivity, resources and systems in place. The shared interest in network and data integrity, privacy and the varied network topographies creates a useful perspective for information sharing between state and local government and private sector partners.

Actively coordinating and collaborating with several Information Sharing and Analysis Centers (ISACs) can be invaluable in the ongoing cycle of threat detection and prevention. The Multi-State ISAC (MS-ISAC) is the focal point for cyber threat prevention, protection, response and recovery for U.S. state, local, tribal and territorial (SLTT) governments. The MS-ISAC maintains a 24x7 cybersecurity operations center that provides real-time network monitoring, early cyber threat warnings and advisories, in-depth vulnerability identification and mitigation and incident response.

Working closely with federal partners at the Department of Homeland Security (DHS), the FBI and the Secret Service, the MS-ISAC also brings the benefit of strong information sharing and relationships with major ISPs, cybersecurity firms, software developers and security researchers. MS-ISAC members share information about their approaches to working with the NIST framework, other cybersecurity initiatives they have underway and the resources that are helping them make progress.

Many opportunities exist for state and local governments to collaborate on cybersecurity, including:

- Working collaboratively to develop a local government overlay for the NIST framework.
- Developing useful metrics on framework implementation based on surveying members.
- Creating tools to promote knowledge sharing among local governments.
- Working on joint initiatives for the National Initiative for Cybersecurity Education (NICE) to help close the cyber workforce gap.

Conclusion

A cyber risk management program cannot completely eliminate risk, but it will do great deal to protect state and local infrastructure and e-Government initiatives more effectively. The critical first step for state and local IT leaders is to assess their institution's specific risks and vulnerabilities. Use risk assessment to proactively realign security strategy around the organization's most valuable assets in context with the most relevant threats. This will increase the efficiency and resilience of your security practice.

The NIST framework, along with ISO 27001, provides helpful guidance and standards, as well as a common language and best practices that government agencies can use to assess their security postures. ISO 27001 outlines risk treatment planning and tailoring appropriate controls to your unique environment. As hybrid IT becomes the norm, additional regulations and standards like FICAM, PCI DSS, HIPAA, and CJIS offer accepted protocols to help state and local governments protect systems and data so they can embrace technological innovation safely and securely. Last but certainly not least, government entities need to share information for stronger security. The more state and local governments engage with federal counterparts and private sector partners, the stronger the fabric for cybersecurity will become across the nation.

For more information, call **(877) 838-7947** to speak to a SecureWorks security specialist.

www.secureworks.com