Risk Management and Compliance for State and Local Governments

In the digital era, information technology has transformed the way state and local governments serve constituents. Heightened connectivity has allowed government agencies to easily and efficiently provide information, enable access to key services, and receive and store sensitive personal data.

However, these benefits are threatened by the actions of cyber criminals intent on breaching government computer networks for political, social, and/or monetary gain. A cyber event such as a denial of service attack attack on a state website can completely disable an IT team's ability to respond and protect constituent data. A more severe incursion that targets computer systems essential for infrastructure and service delivery can potentially wreak havoc on entire swaths of the economy and even endanger citizens.

In light of these risks, cyber security has never been more important. Yet, a recent NASCIO survey found that state and local governments are woefully unprepared to deal with an attack on their networks.[1] In general, the survey revealed that government agencies are failing to keep up with increases in threats; lack a regularly updated security program with defined reporting processes; lack appropriate levels of management or executive support; and have yet to develop adequate privacy controls.

State and local agencies must focus on ensuring that confidential and sensitive data is protected and that they can respond quickly and effectively to a breach. They must be able to understand what is under attack and respond in as near real time as possible. Finally, they must be able to reassure the public that government systems and data are secure. To achieve these goals, government agencies must employ a dynamic, layered approach that strengthens the cyber security of their networks and systems.

The Department of Homeland Security's automated risk management and compliance initiative—which they call the Continuous Diagnostics and Mitigation Program, or CDM—dictates best practices and programs to address cyber threats. In essence, the program stresses that states can no longer afford to take point-in-time assessments to determine the level of risk in an environment. Instead, government agencies must implement solutions that leverage sophisticated analytics to offer near real-time assessment so that they can understand, prioritize, and mitigate risks as they arise.

RISK MANAGEMENT AND COMPLIANCE BEST PRACTICES

A strong risk management and compliance solution or suite of solutions provides the detection and prevention controls to effectively protect government infrastructure from cyber warfare. Preventative controls encompass authentication, authorization, access control, server protection, protected communications, encryption, and security awareness. Detection controls include virus detection, intrusion detection, data loss prevention, audit, backup and recovery, and incident response. First, however, the following risk management and compliance best practices should be implemented.

Compliance Automation

Many governance, risk, and compliance processes can be automated, resulting in improved operational efficiency, higher constituent satisfaction, reduced data loss, and lower compliance costs. These solutions improve visibility into the organization's level of risk. With that information, IT can prioritize risks and identify efficient, cost-effective remediation efforts.

IT Risk Management and Continuous Monitoring

A risk management and compliance solution's primary function is to help government IT communicate risk in business-relevant terms. By leveraging common compliance frameworks and robust data metrics, IT can produce a risk-based view of the government IT infrastructure. A solution capable of receiving such data metrics is crucial. Analytics that measure risk are particularly important to government agencies because they offer an effective way to reassure the public that their systems and data are secure.

1 *The 2014 Nationwide Cyber Security Review (NCSR)*

Managed Security Services
A world-class security partner offering managed services can build and sustain a resilient incident management program in the face of increasingly sophisticated attacks and malware variants. Comprehensive management of the security infrastructure should include log management, monitoring, and analysis of security posture and events. Customer options may include on-premise, hosted service, or off-premise solutions based on preference.

Metrics
Encryption, data loss prevention, and endpoint management—three common and powerful security tools—contain high value data that most organizations today can only see in silos. A comprehensive risk management and compliance solution that leverages data from these sources can provide a true view of risk for the organization, enabling valuable prioritization and remediation. The following highlighted IT security functions or solutions can feed appropriate metrics to the tool:

- ***Encryption***—Once IT has discovered all IT assets that must be protected, as well as all vulnerable endpoints, and established policies that dictate what should and shouldn't be encrypted, an encryption solution can be chosen. Advanced disk, data, and file encryption can protect PCs, laptops, mobile devices, removable drives, servers, file shares, and emails from unauthorized access. A solution with a central management console enables safe, central deployment and manages encryption at all potential endpoints.

- ***Data Loss Prevention***—More and more attacks start by targeting individual employees through social networking. Data loss prevention is needed once the organization understands its goals and priorities and has established roles and responsibilities. A comprehensive risk management and compliance approach includes a data security solution that discovers, monitors, protects, and manages confidential data wherever it is stored or is in motion. These solutions work most effectively from a unified, web-based management platform.

- ***Security and Endpoint Management***—Risk management best practices include the ability to discover and inventory all hard and soft IT assets in an organization, to protect discovered devices from malware and zero-day threats, and to deliver new software and patches to vulnerable systems. Automation of these processes is key to delivering a stable, secure, and managed environment. Such solutions must provide sufficient reporting and analytics to empower data-driven decisions regarding the IT environment that align with organizational objectives.

SYMANTEC RISK MANAGEMENT AND COMPLIANCE SOLUTIONS FOR STATE AND LOCAL GOVERNMENTS

Automated risk management and compliance solutions help government institutions align priorities across security, IT operations, and compliance. With these solutions, government agencies can harden the data center, prioritize security remediation, enable secure migration to the software-defined data center, and support continuous assessments and monitoring to ensure cyber security. Symantec helps state and local government organizations maintain secure 24x7 operation of critical IT systems and protect government and citizen data from loss, malware, or breach. Symantec solutions automate processes to meet a variety of national compliance needs, as well as state privacy law requirements.

More Information
Visit our website
www.symantec.com
To speak with a Product Specialist in the U.S.
1 (800) 745 6054

About Symantec
Symantec Corporation (NASDAQ: SYMC) is an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to *www.symantec.com* or connect with Symantec at: *go.symantec.com/socialmedia*.

Symantec World Headquarters
350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com