Don’t MSS With Texas:

How Managed Security Services Improves Texas Statewide Cybersecurity Posture

Cybersecurity Category Submission
State of Texas

Nancy Rainosek, Chief Information Security Officer
Texas Department of Information Resources
300 West 15th Street, Suite 1300
Austin, TX 78701

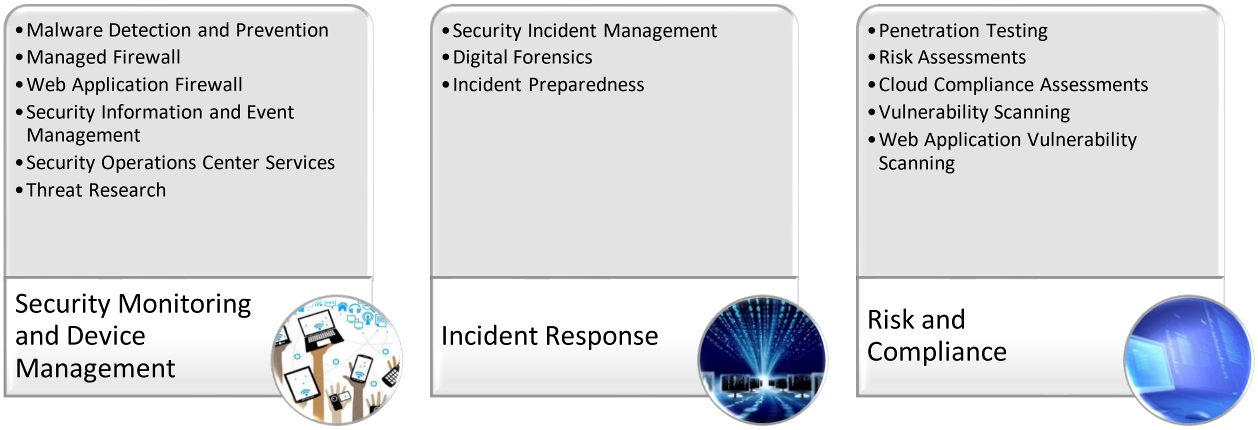
Project Initiation	November 2017
Project Completion	April 2018

DIR
Texas Department of Information Resources

Executive Summary

IT Security is an increasingly critical priority for state and local governments, demanding heightened awareness of malicious threats and an expanded focus on the technologies protecting sensitive information. In addition to ensuring secure computing environments, government entities are under never-ending requirements to meet rising constituent needs, do more with less, and increase the value they deliver to the public. In addition, the demand and competition for qualified cybersecurity professionals is alarming, and the problem is expected to increase. Cybersecurity Ventures predicts there will be 3.5 million cybersecurity job openings by 2021.[1]

To meet these needs, the Texas Department of Information Resources (DIR) introduced Managed Security Services (MSS) as a new offering within its Shared Technology Services program to provide uniform and consistent management of state data security at affordable rates. The MSS program was developed to leverage statewide resources to provide cost-efficient security services to state, local, municipal, local school districts, higher education and other eligible organizations. MSS assists DIR Customers in consolidating security services, meeting legislative security requirements, mitigating security risks, and filling gaps in skillsets to provide a secure computing environment for their business and to deliver more effective services for their constituents.



- Malware Detection and Prevention
- Managed Firewall
- Web Application Firewall
- Security Information and Event Management
- Security Operations Center Services
- Threat Research

Security Monitoring and Device Management

- Security Incident Management
- Digital Forensics
- Incident Preparedness

Incident Response

- Penetration Testing
- Risk Assessments
- Cloud Compliance Assessments
- Vulnerability Scanning
- Web Application Vulnerability Scanning

Risk and Compliance

Figure 1: MSS Services Listing

MSS is comprised of three service categories: Security Monitoring and Device Management, Incident Response, and Risk and Compliance. A listing of the services is shown in Figure 1.

In just over a year since implementation, more than 70 customers have requested nearly $4 million on MSS engagements, indicating the need and desire for the services. In addition, because this program leverages significant volume discounts, customers save between 30-40% on their services, allowing them to more efficiently utilize their limited resources.

Total MSS Spend in First Year
(March 1, 2018 – March 31, 2019)

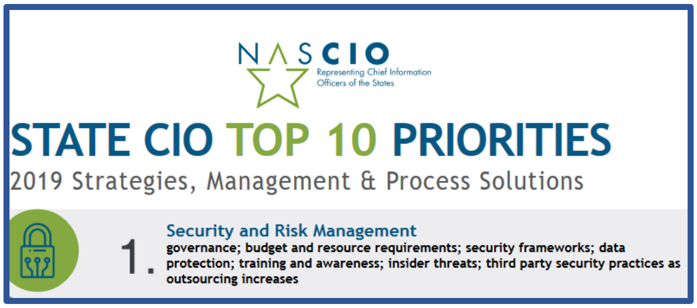
$3.98 Million

Figure 2: Total MSS spend as of March 31, 2019

[1] https://cybersecurityventures.com/jobs/

Concept

Cybersecurity has become a high priority nationwide, leading the list of state CIO's top priorities in a 2019 NASCIO survey. Texas has also placed a significant focus on security initiatives, knowing that the state is an attractive target for attackers. The number one goal in the Texas State Strategic Plan for Information Resources is to provide reliable and secure services and the Texas Legislature also views cybersecurity as a priority, passing several bills relating to protecting state assets.



NASCIO Representing Chief Information Officers of the States

STATE CIO TOP 10 PRIORITIES

2019 Strategies, Management & Process Solutions

1. Security and Risk Management
governance; budget and resource requirements; security frameworks; data protection; training and awareness; insider threats; third party security practices as outsourcing increases

Figure 3: NASCIO State CIO Top 10 Priorities 2019

With this increased focus, state and local government organizations are being asked to do more to protect their IT assets and data with the same number of resources. As a federated state government, each agency is responsible for the security of their information resources. So, while larger organizations may have the ability to implement the necessary tools and hire more qualified staff to mature their security program, smaller entities are often unable to dedicate staff and funds to accomplish this.

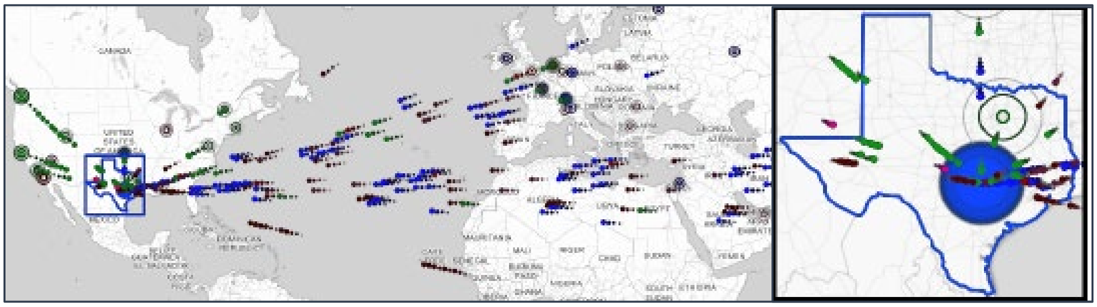


Figure 4: Texas Threat Map. In a moment's time, Texas faces hundreds of cyberattacks from all over the world.

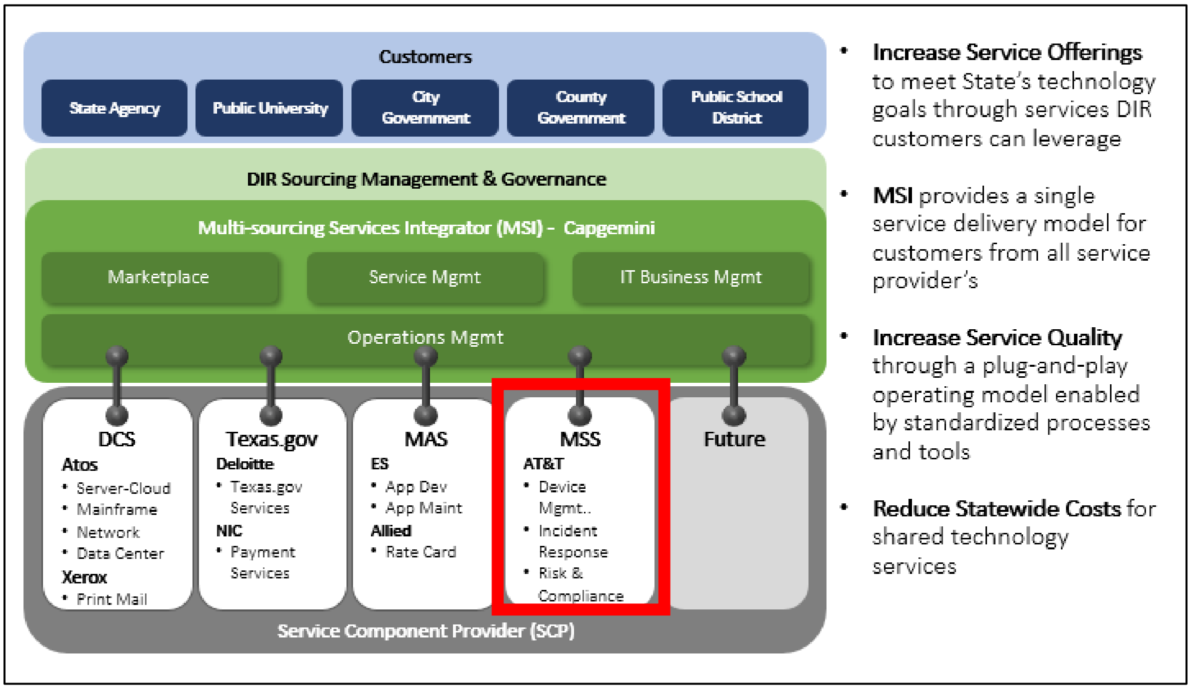
In an effort to bridge this gap, the DIR started assisting state agencies and institutions of higher education by providing penetration testing (in the early 2000s) and security assessments (in 2011). Prior to the MSS program, every organization was required to complete administrative and contractual agreements before obtaining each service. The granular nature of the process combined with the volume of demand for services created an administrative burden on DIR staff and resources.

The success of the penetration testing and security assessments at the state level led to an increased interest by local governments and other public sector entities in DIR service offerings. Unfortunately, funding restrictions limited these services to state agencies and public institutions of higher education. To fulfill a truly statewide approach to information security, DIR considered all 254 counties along with thousands of cities, school districts and quasi-governmental organizations.

To answer this need, DIR implemented the Managed Security Services (MSS) Program to facilitate providing security services for Texas public sector organizations. These security services assist state agencies, local and municipal governments, local school districts and higher education entities in meeting legislative requirements, mitigating security risks, and filling gaps in skill sets necessary to provide a secure computing environment using fewer resources. This enables the state to provide security services to Texas constituents in a more effective and efficient manner.

Significance

Implemented in March 2018, DIR now provides MSS through its Shared Technology Services (STS) program. STS delivers proven, scalable, integrated Information Technology services to solve the business problems of the state agencies, institutions of higher education and local governmental entities. The structure of the STS Program is shown in Figure 5.



- **Increase Service Offerings** to meet State's technology goals through services DIR customers can leverage
- **MSI** provides a single service delivery model for customers from all service provider's
- **Increase Service Quality** through a plug-and-play operating model enabled by standardized processes and tools
- **Reduce Statewide Costs** for shared technology services

Figure 5: Shared Technology Services Program Structure

The Shared Technology Services program is managed by the Multi-sourcing Services Integrator (MSI) which provides a next-generation digital platform for service providers and customers. The platform includes services level management, service desk support, constituent help desk support, program management, business continuity, disaster recovery testing and planning, marketplace functionality, performance analytics, and financial management. This centralized platform includes a Shared Technology Services Customer Portal which provides a secure, single point of access to the marketplace, tools, reports, data, newsletters, contacts, governance committee meeting documentation, enterprise calendars and other useful information.

As a service offering through Shared Technology Services, the MSS program is divided into three different service components: Security Monitoring and Device Management, Incident Response and Risk and Compliance.

The services offered in the MSS program include the following:

Security Monitoring and Device Management

Malware Detection and Prevention Systems
Malware Detection System (MDS) and Malware Prevention System (MPS) services is a fully managed security solution for recognizing and responding to malware in the customer network environment.

Security Monitoring and Device Management (Continued)

Managed Firewall Services

Managed Firewall Service provides a highly functional layer of security to customer networks. The service is a fully managed solution, which includes all hardware and software components, configuration, installation, day to day management and maintenance, as well as expert customer support and proactive network monitoring.

Web Application Firewall (WAF) Services

Web Application Firewall (WAF) is a form of firewall which controls access to web applications by monitoring and potentially blocking web traffic which does not meet the configured security policy requirements for the web application.

Security Information and Event Management (SIEM)

The Security Information and Event Management (SIEM) solution delivers a real-time understanding of the world outside—threat data and reputation feeds—as well as a view of the systems, data, risks, and activities inside the customer enterprise.

Security Operations Center (SOC) Services

The Security Operations Center (SOC) service is a fully managed service customized to meet your specific needs for security operations. This service is intended for customers who do not have a security operations center, or customers who already have a SOC and want to augment their operations with help from a service provider.

Threat Research Services

Threat Research is focused on identifying global threats and applying that understanding to the data and information developed and captured at the local level. Threat Research is a complement to the SIEM and Log Management Services, but it can be valuable even as a stand-alone service.

Incident Response

Security Incident Management

Incident Management services provides expert assistance to you in the event of a security breach. This service enables you to field a team of information security professionals in response to a security incident or breach, assess the nature and depth of the breach, and remediate the breach.

Digital Forensics

Digital Forensics is the detailed technical analysis that supports the root cause of an incident. This service provides customers access to skilled technicians who are able to perform a unique type of data analytics needed for Root Cause Analysis and remediation.

Incident Response Preparedness

Incident Response Preparedness uses an industry leading incident management framework coupled with the Service Provider’s experience to will assess the current status of the customer’s incident management program and develop a future state of the incident program and associated roadmap based on the framework.

Risk and Compliance

Penetration Testing
Penetration Testing services use a tested methodology to identify vulnerabilities for exploit, and to exploit the most critical vulnerabilities to gain unauthorized and elevated levels of access within a customer's environment.

Risk Assessments
Risk Assessments focus on the maturity of processes, gaps against standards of good practice and compliance requirements, and risks to the organization.

Cloud Compliance Assessments
A Cloud Compliance Assessment is a review of security policy enforcement employed by third parties, cloud providers, and service providers.

Vulnerability Scanning Services
The Vulnerability Management service is used to conduct host discovery or vulnerability scans on external or internal IP-based systems and networks. The technology employs a variety of scanning techniques to survey the security posture of the target IP-based systems and networks.

Web Application Scanning Services
The Web Application Vulnerability Scanning service is used to conduct application validation and discovery or Web Application Vulnerability scans on external or internal applications.

The MSS offers several benefits to the Texas public sector community. First, customers that were already a part of the Shared Technology Services program were able to take immediate advantage of MSS beginning on March 1. Second, customers sign an agreement to participate in Shared Technology Services one time, and that agreement does not expire. All future engagements can be self-requested through the customer portal.

Finally, and possibly one of the greatest benefits of MSS is that many other types of customers can participate and leverage the buying power of the state. Not only can state agencies and universities participate, but now county, city and municipal governmental entities, along with school districts, can purchase MSS services.

Impact

In its inaugural year, the MSS program has delivered several key benefits to the Texas public sector. First and foremost, the MSS program has helped its customers meet legislative requirements, mitigate security risks, and fill gaps in hard to find skillsets.

The MSS program provides an option for customers who want to outsource certain parts of security services depending on each customer's need. The MSS service component provider can also add or customize services quickly based on customer need and demand.

Regarding incident management services, the MSS program provides 24x7 availability for incident response staff via an always available project bench of security subject matter experts, and MSS customers do not need to pay a retainer for incident management services, resulting in immediate cost-savings.

When looking at MSS from a process perspective, adding it to the STS Program brought forth several immediate benefits. DIR provides an ITIL services integration layer (the MSI) for standard service delivery and financial chargeback, as well as other centralized management functions. This provides a consistency of services through MSI oversight, provides standardized hardware and software across customers and reduced paperwork for DIR-funded services.

From a procurement perspective, the MSS Program has the added benefit of being competitively procured at the statewide level, with DIR performing vendor management and oversight, which minimizes the procurement and contractual overhead of the customer organizations.

In late 2018, the Texas Secretary of State received Help America Vote Act (HAVA) funds to assist with securing state elections systems. Using the MSS, DIR and the Secretary of State worked closely with the service provider to add customized assessments for all components around elections systems as a service. The Secretary of State is offering these assessments to all Texas counties and will be working with the MSS service providers to determine remediation actions. This highly visible project was in progress and assessments were began approximately six months after DIR was approached by the Secretary of State. Had the MSS Program not been utilized, the time needed to start the project would have been extended and assessments may not have been completed in the required timeframe.

Finally, MSS offers significant cost savings to customers. When compared to market rates for similar services, customers see the following savings:

35%

Discount rates for Security Monitoring and Device Management (average over all the services)

40%

Discount rates for Incident Response Services. Also, no retainer for Incident Management Services.

30%

Discount rates for Risk and Compliance (40% discount for penetration tests)

In summary, the threat landscape for Texas is constant and ever-growing. Public sector organizations are being asked to fight a cybersecurity war with few resources, and to consistently do more with the same or less. With the implementation of the MSS Program, Texas is now leveraging buying power to provide expert security services to not just state-level organizations, but to smaller local governmental entities. This innovative program has changed how cybersecurity can be done in the state of Texas by offering a wide variety of services and products to help defend against the cyber threat landscape head-on, and at substantially discounted rates. We face the future ready to protect and defend our information and resources. Don’t MSS with Texas!