Peraton

WHITEPAPER

MANAGED CYBERSECURITY SERVICES

EXECUTIVE SUMMARY

Organizational leaders are fast discovering how digital transformation benefits their mission critical programs and business processes. Multitasking remote workers are increasingly teaming virtually, any time and from anywhere, confidently and safely leveraging efficient cloud platforms to achieve timely results. Data scientists now apply AI/ML capabilities to swiftly discern actionable trends from oceans of collected data. Technologists exploit autonomous processes to streamline previously labor-intensive tasks. Watch standers respond decisively to enterprise threats revealed in real-time on single pane displays for hyper situational awareness. These and many other welcome transformations help enable modern work environments. However, they demand high performance from the organization's cyber and information technology professionals.

Chronic shortages of expert staff, burdensome upkeep of unsafe legacy infrastructure, and overtasked program managers with little bandwidth or resources to apply to new initiatives challenge even the most dedicated teams. Additionally, the need for reliability, resilience, and security has never been greater. The audacity of sophisticated cyber actors spying on sensitive programs, disrupting business processes, or extorting fees for ransomed data increases with every successful compromise. Still, the future is bright as we are in this together. Information sharing and cooperation among partners—federal, state, local and tribal governments, the private sector, academia, as well as our international allies—will be key to our mutual success in navigating the digital road ahead.

On May 12, 2021 the Biden administration issued a new executive order (EO)[1] to enhance our nation's cybersecurity posture which notably includes coordinating partnerships with the private sector to support the EO execution. The EO represents a significant number of activities that will require directed actions and significant effort among all U.S. federal government agencies and government contractors/ subcontractors.

The new EO requirements make cybersecurity and securely managing government data more important than ever before. Peraton welcomes this opportunity to further our trusted partnership with the Federal Civilian Executive Branch (FCEB) agencies, Department of Defense (DOD), and the Intelligence Community (IC) in support of their mission accomplishment. This whitepaper highlights Peraton's capabilities that can directly enhance implementation of the EO.

[1] Executive Order on Improving the Nation's Cybersecurity (May 12, 2021) Presidential Actions

MANAGED CYBERSECURITY SERVICES: CHALLENGES AND BEST PRACTICES

U.S. federal, state and local government executives are keenly focused on protecting vital data assets, ensuring data privacy and creating information resilience to combat cyberattacks by nation states (China, Russia, North Korea and Iran), cyberattack groups, criminal cyberattack groups and hacktivists. According to the Ponemon Institute's 2019 Economic Study of Security Operations, security operation centers (SOCs) are considered critical in detecting cyberattacks and are core to most cybersecurity strategies, with 73% of the respondents stating that SOCs are essential or very important to their overall cybersecurity strategy.

This white paper addresses key questions and outlines the benefits of outsourcing of cybersecurity services. Peraton's proven, effective cybersecurity managed services best practices are shared along with a pertinent federal agency case study.

Why outsource cybersecurity services?

Said simply, organizations are increasingly choosing to outsource cybersecurity services because it provides better, faster, and more effective protection. For many years, federal, state and local governments have struggled with the complex, multifaceted challenge of protecting critical information assets including classified information (CI), intellectual property (IP), personal identifiable information (PII), protected health information (PHI), controlled unclassified information (CUI) and other sensitive information (SI). The skyrocketing number of cyberattacks and increasing levels of sophistication including insider threat attacks, supply chain cyberattacks, business email compromise (BEC) attacks, ransomware attacks, distributed denial of service (DDoS) attacks, brute force attacks, advanced persistent threat (APT) malware attacks and spear phishing attacks, can make it challenging for an agency to keep up with best practices and adequately manage cybersecurity services in-house.

What are the key factors in deciding to outsource cybersecurity services?

To perform essential, effective cybersecurity functions and services internally, agencies need to hire information technology (IT) personnel and invest in the hardware, software, facilities, education and training needed to protect their critical data assets. Alternatively, agencies can choose to outsource the IT services and related information security services to a government contractor.

This traditional procurement "make or buy decision"—often referred to as an outsourcing decision—can be quite challenging given the factors that need to be considered:

- Total cost of ownership (TCO) insourcing versus outsourcing—facilities, hardware, software, employees, education/training, retention of resources and professional support services
- Availability of IT and related cybersecurity talent in a highly competitive market
- Qualification of security personnel—education, experience, professional certifications and security clearances
- Resource/labor continuity
- Facilities security considerations
- Level of performance concerns
- Ability to adapt to evolving cyber threat landscape
- Limitation of liability or damages issues
- Business continuity planning/back-up facility
- Disaster recovery planning

What is a managed security services provider (MSSP)?

An MSSP is an organization that provides a variety of outsourced information security services for information systems, networks, email, software applications and endpoints. MSSPs typically operate on a continuous—24/7/365—basis with a robust SOC at the heart of their organization. The SOC is usually staffed in a three-tier organizational structure operating on a two 12-hour shift basis or three eight-hour shift basis. The purpose of an MSSP is to provide continuous, high quality cybersecurity services for a customer organization.

What are the five key questions a government agency should ask an MSSP?

Government agencies should consider asking an MSSP the following questions prior to vendor selection:

- How will the MSSP's services scale up or down to meet your changing needs?
- How will insider threats be detected?
- Does the MSSP's service monitor to the endpoints 24/7/365?
- How does the MSSP gather threat intelligence?
- What is the MSSP's pricing model?

What are the major benefits of an MSSP?

There are numerous proven benefits for a government agency to use an MSSP for their cybersecurity services:

- Turnkey information security operation with continuous quality cyber protection services
- Potential reduction in security-related hardware and software costs
- Access to industry knowledge and threat intelligence as appropriate
- Increased labor efficiencies and workflow automation that can reduce the number of operational security personnel your agency needs to hire, train and retain to maintain an acceptable security posture

What are the common MSSP services?

Common MSSP services include:

- SOC monitoring, analysis and management
- Security information and event management (SIEM)
- Managed firewall and cyber perimeter defense
- Cybersecurity governance, risk and compliance (GRC)
- Identity credential and access management (ICAM) systems and services
- Data privacy
- Cloud security
- Intrusion detection systems (IDS)
- Vulnerability management
- Penetration testing
- Security dashboard systems and services
- Incident response

What are the major business challenges when transitioning to managed cybersecutiy services?

Many agencies have decided to transition from internally managing information security using their own employees or a combination of internal employees and government contractors, to a comprehensive managed cybersecurity services model provided by a qualified MSSP. Typically, when government agencies transition to a managed cybersecurity services model they encounter several significant business challenges:

- Develop a new performance-based cybersecurity acquisition strategy to acquire a more effective cyber defense
- Determine how to incorporate an innovation process into a managed services contract (adding/replacing systems and tools)
- Select a vendor system/software/tool-agnostic MSSP
- Establish operating level agreements (OLAs) with other IT contractors who perform related IT and cyber work
- Develop and negotiate appropriate cybersecurity managed service level agreements (SLAs), key performance indicators (KPIs), performance metrics, acceptable quality limits (AQLs) and performance incentives/disincentives
- Determine how to best leverage legacy information technology (IT) infrastructure, cloud infrastructure and software applications to enhance enterprise cyber defense
- Ensure compliance with a vast number of information security and data privacy regulatory requirements
- Ensure cloud access security and endpoint protection
- Reduce operational costs via automation, data analytics and artificial intelligence applications
- Enhance cyber situational awareness and provide mission assurance via data resilience

PERATON'S MANAGED CYBERSECURITY SERVICES AND BEST PRACTICES

Peraton offers eight proven, effective managed cybersecurity services best practices:

Consider key MSSP capabilities including:

- Continuous monitoring, level of visibility and coverage—some managed services limit their coverage to a specific vendor or infrastructure
- Integration with existing sensor—managed security services need to work with existing sensors where possible
- Level of automation—using software to automate the role of level one and some level two SOC analysts provides faster response time and better scalability
- Insider threat detection—MSSPs must provide the right data analysis to help you take the appropriate action to thwart insider attacks
- Integration with an IT services management platform—providing full services integration of risk management, vulnerability management, vendor risk management and incident response to provide better and faster situational awareness and governance, risk and compliance documentation for continuous authorization to operate (ATO)

Verify the MSSP meets or exceeds the following information security standards and guidance:

- Federal information Security Modernization Act of 2014 (FISMA2014)
- National Institute of Standards & Technology (NIST) FIPS Publication 140-3, Security Requirements for Cryptographic Modules
- NIST FIPS Publication 197, Advanced Encryption Standard (AES)
- NIST FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems
- NIST FIPS Publication 200, Minimum Security Requirements for Federal information and Information Systems
- NIST FIPS Publication 201, Personal Identity Verification (PIV) of Federal Employees and Contractors
- NIST Special Procedure (SP) 800-37, Rev. 2, Risk Management Framework for Information Systems and Organizations
- NIST SP 800-40, Guide to Enterprise Patch Management Technologies
- NIST SP 800-51, Guide to Using Vulnerability Naming Schemes
- NIST SP 800-53, Rev. 5, Security and Privacy Controls for Information Systems and Organizations
- NIST SP 800-61, Rev. 2, Computer Security Incident Handling Guide
- NIST SP 800-82, Rev. 2, Guide to Industrial Control Systems (ICS) Security
- NIST SP 800-83, Guide to Malware Incident Prevention and Handling for Desktops and Laptops
- NIST SP 800-92, Guide to Computer Security Log Management
- NIST SP 800-122, Guide to Protecting the Confidentiality of Personal Identifiable Information (PII)
- NIST SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
- NIST SP 800-171, Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations
- NIST SP 800-207, Zero Trust Architecture

Ensure the MSSP provides managed detection and response (MDR) services

It is vital that the MSSP be able to provide MDR services on a 24/7/365 basis. Typically, MDR services include cyber threat intelligence services, continuous threat monitoring, detection and incident response services to customers. MDR providers usually leverage a combination of technologies deployed at the host and network layers, advanced data analytics, threat intelligence and human expertise in incident investigation and response.

Select an MSSP which offers expanded/optional cybersecurity services

Ideally, it is best to select an MSSP which offers a comprehensive portfolio of cybersecurity services that provide a one-stop shop for their information security requirements. Key expanded or optional services include:

- Third Party Assessor Organization (3PAO) capabilities to assess software applications and cloud security for FedRAMP certification
- Zero trust architecture (ZTA) planning and system integration services
- Identity credential and access management (ICAM) planning and system integration capabilities
- A certified provider of ITIL information technology and cybersecurity education and training programs

Create service performance metrics in the MSSP contract

Create and incorporate mutually agreed-upon KPIs with related performance standard threshold (PST) and an acceptable quality level (AQL) into the MSSP contract. For example:

KPI	PST	AQL
Availability/uptime	99.5%	Greater than or equal to 99.5%
MSSP outage event notification	Within 10 minutes	Less than 10 minutes
Incident response time	Within one hour of incident detection	Less than one hour

Structure the MSSP contract as a fixed-price agreement with options and discounts

Most MSSPs offer a fixed-price per month for their defined security services on an annual contract basis, with priced options for each additional year of service. Typically, the longer the period of performance, the larger the discount on the security services.

Require the MSSP to implement Security Orchestration Automation and Response (SOAR) technology

Many of the leading MSSPs are now implementing SOAR technology. This technology offers an advancement in the level of system integration of the SIEM system (e.g., Splunk or ArcSight with vulnerability scanning information and threat management data)—leveraging artificial intelligence, automation, data analytics and security data visualization tools.

Execute a performance-based acquisition (PBA) acquisition strategy to select the MSSP

Develop a new enterprise cybersecurity managed services acquisition strategy based upon a PBA model including:

- Performance work statement (PWS)
- Performance metrics
- Performance standards/SLAs
- KPIs
- Performance incentives
- AQL services requirements

Request that government contractors develop proposals to help your agency transition from the current cyber staffing and internal management model to a new managed cybersecurity services model via a time-phased approach. Include a requirement in the request for proposal (RFP) for the MSSP to be cyber system and software vendor platform agnostic to ensure the best possible/most customer appropriate selection of cybersecurity tools.

Case study: Government Enterprise Cybersecurity as a Service (CaaS)

Peraton has successfully used the PBA acquisition strategy with a large civilian agency over a seven year time frame to transition from cyber staff augmentation to managed cybersecurity services using government-provided facilities and government-selected cybersecurity tools. Our outstanding performance results for the CaaS program create an excellent enterprise managed cybersecurity services case study for federal, state and local agencies to consider.

We have provided secure delivery of services to the agency's customers by implementing cybersecurity best practices and ensuring compliance with federal, NIST, agency and related IT/cybersecurity policies, regulations and directives within the IT infrastructure. Implementing the Peraton CaaS approach, the government agency has significantly reduced operational risk and improved enterprise cyber defense performance results through enhanced automation, integration and advanced data analytics.

The managed security services contract required the phased transition from cyber staff augmentation on a level-of-effort (LOE)-basis to a performance-based contract—including a PWS, AQLs and an disincentives plan—to implement a comprehensive enterprise portfolio of cybersecurity managed services, CaaS. The Peraton CaaS approach allows the government to scale systems and services up or down as needed with a flexible pricing model based upon the level of consumption of cybersecurity services.

The managed cybersecurity services CaaS contract scope of work includes:

- SOC
- Information System Security Officer (ISSO)
- GRC
- Communications Security (COMSEC)
- Cybersecurity engineering
- Configuration management
- Information assurance
- Cloud security services
- FedRAMP support services

CaaS program key facts:

- Consists of over 125 operational FISMA systems
- Enterprise deployment of Splunk SIEM
- Implementation of continuous diagnostics and mitigation (CDM)
- Implementation of SOAR
- Penetration testing systems and tools
- Established ongoing ATO with common controls program
- Serve as FedRAMP subject matter experts for all agency cloud systems

SUMMARY

Federal, state and local government agencies need cost-effective, highly qualified managed security services to safeguard government networks, email systems, software applications and endpoints. Regardless of the size and maturity of your SOC, when considering the evolving complexity of the cyber threat landscape, managed cybersecurity services may be an advantageous choice for your agency.

Peraton

Learn more at

PERATON.COM