STRENGTHENING CYBERSECURITY THROUGH MANAGED SERVICES

Executive Summary

Some core organizational services are complex to implement in terms of the technologies, skills, or applicable regulatory requirements making these impractical for agencies to implement in-house. Therefore, access to shared service providers by federal Government agencies is critical to providing access to services, improving service delivery, and driving cost-efficiency. The federal Government has established the framework for governing shared service centers, but it is up to individual agencies to build and operate the shared service center. This paper summarizes the challenges and provides recommendations for operating a successful shared service center.

Introduction

Implementing a shared service center in a federal agency is not just a matter of consolidating operations, but requires a cultural transformation of the organization. The agency must align its organizational structure, technology, and funding to support this specific service delivery model. The creation of a shared service center demands a unified governance framework that balances the needs of multiple agencies while maintaining clear lines of accountability between each program.

Problem Statement

Many agencies find it challenging to establish clear performance benchmarks and consistent management structures for cybersecurity programs. The issue is exacerbated when each agency has its own set of expectations and regulatory requirements. Typically, service providers also require a unified technology infrastructure that is suited to the delivery of multiple distinct customers in a consistent and efficient manner and introduces the need for special muti-tenant considerations related to each technology platform involved in the delivery of services. In summary, the broader challenge with implementing a shared service center in a federal agency lies in orchestrating complex organizational change, which deals with overcoming entrenched cultural barriers, setting up robust governance and funding mechanisms, and integrating legacy technologies under stringent security and compliance frameworks. Each of these elements is interdependent, and success in one area often hinges on progress in another.

Cybersecurity shared service providers must be able to address these challenges while supporting customers, marketing and selling to new customers, and keeping the Department safe and secure. The cybersecurity shared service provider must also account for oversight activities and requirements. Federal shared service centers are formally approved and overseen by a Quality Service Management Office (QSMO), established under Office of Management and Budget (OMB) guidance, which is responsible for defining and overseeing the implementation of standardized and high-quality support services across the Government. The Cybersecurity and Infrastructure Security Agency (CISA) within the Department of Homeland Security (DHS) is designated as the cybersecurity QSMO, and is responsible for ensuring that federal agencies can access consistent and effective cybersecurity solutions through a centralized marketplace.

Proposed Solution / Approach

Federal agencies need to be able to supplement their existing cybersecurity expertise with managed or shared services expertise to succeed and excel as cybersecurity shared service providers. The ability to deliver cybersecurity services under the shared service model requires a thoughtful, well-designed governance model that implements and enforces the mechanisms required to address the challenges noted throughout this paper. Some key elements include:

Service Architecture: Designing, modifying, and delivering shared services to customers involves a dynamic, customer-centric approach. This begins with mapping the entire customer journey to identify and address key customer outcomes, and then developing clear and standardized processes to ensure consistent operations. Metrics should also be accounted for at the outset to inform service performance for the provider and to offer potential service delivery objectives that customers may want or need to formally capture in Service Level Agreements (SLAs) or Experience Level Agreements (XLAs).

Change management: While agencies typically have change management in place related to IT systems, in the context of a shared service provider, this means managing changes to services. Complementary to Service Architecture, any planned changes to services must be implemented through an effective Change Management practice in order to minimize risk of disruption regardless if the service changes are to add, modify, or deprecate the services that are offered. Innovation is critically important to shared service providers, and effective Change Management is required to foster innovation.

Financial Management: Shared service providers must be able to break down and account for all of the cost factors associated with the delivery of an individual service. This is used to develop a cost model for each service, which ensures accuracy and transparency in support of chargeback to customers. This is a unique practice and skillset, which agencies must be able to address.

It's important to note that agencies not operating shared service centers can benefit from integrating the same fundamental elements into their cybersecurity programs to drive transparency, cost efficiency, and effectiveness. This is especially true for organizations operating at the Department-level, which have responsibility and accountability for the security program across the entire Department, and in essence, operate as shared service providers for their numerous constituent agencies.

Our Team, Your Advantage

Tyto Athene is not just a technology provider—we are a trusted mission partner with unparalleled experience and expertise in delivering successful shared services. The following graphic captures some of the key experience we have that can directly benefit customers.

SOC as a Service (SOCaaS)

We've helped the Department of Justice (DOJ) design, implement, and operate its Cybersecurity Shared Services Program (CSSP), which delivers SOCaaS to federal agency customers. DOJ's SOCaaS was accredited as a Center of Excellence by DHS and awarded "Gears of Government" recognition by the Chief Information Officers Council.

Managed Zero Trust Network Access

Under DOJ's CSSP, we also led the design and implementation of the Justice Edge Trust Service (JETS), a fully managed Zero Trust Network Access (ZTNA) solution providing comprehensive security capabilities for CSSP customers.

DOD365 Integrated Phone System (DIPS):

As the leading voice provider for the Department of Defense (DoD), Tyto Athene's DIPS solution enables warfighters, defense personnel, and mission partners to leverage Microsoft Teams for voice calls and Direct Inward Dialing (DID) to or from any global number streamlining communication regardless of physical location. The system supports up to 360,000 concurrent calls via low-latency, high-bandwidth telephony ensuring fast, reliable voice connections. The service is designed with global full redundancy and automatic failover, as well as end-to-end encryption.

For more information about our cybersecurity services, please email bd@gotyto.com

https://gotyto.com

Tyto GSI is registered in System for Award Management (SAM) as a Large Business under NAICS Code 541519.

TYTO Athene

DATA TO DOMINANCE