



ISOAG May 1, 2019 Agenda

- | | |
|--|------------------------------|
| I. Welcome and Opening Remarks | Mike Watson, VITA |
| II. Cybersecurity and Infrastructure Security Agency Overview | Benjamin Gilbert, DHS |
| III. Working Effectively With Security Stakeholders | Amy Luffey, ABC |
| IV Security Operations Update | Bill Stewart, VITA |
| V. Upcoming Events | Mike Watson, VITA |



Virginia Information Technologies Agency

**There are no slides available from our
speaker
Benjamin Gilbert**



Working Effectively with Stakeholders and Conflict

Amy Luffey

May 1, 2019

*Gartner: A practical Guide To Stakeholder Management, H. Colella & A. Rowsell-Jones, August 2018;
Harness the Power of Conflict to Fuel Collaboration, R. Handler, August 2015*

Overview

- Define Stakeholder
- Identify Critical Success Factors
- Review Strategies and Tactics
- Address Conflict

Stakeholder Defined

A person with an interest or concern in something, especially a business

Critical Success Factors

- Ability to accurately & completely identify stakeholders
- Ability to manage stakeholder influence
- Ability to effectively communicate with stakeholders

Identify Stakeholders By Role

- Responsible for getting the work done
- Accountable for the outcomes or results of the work
- Consulted while the work is being created
- Informed along the way
- *Observer*

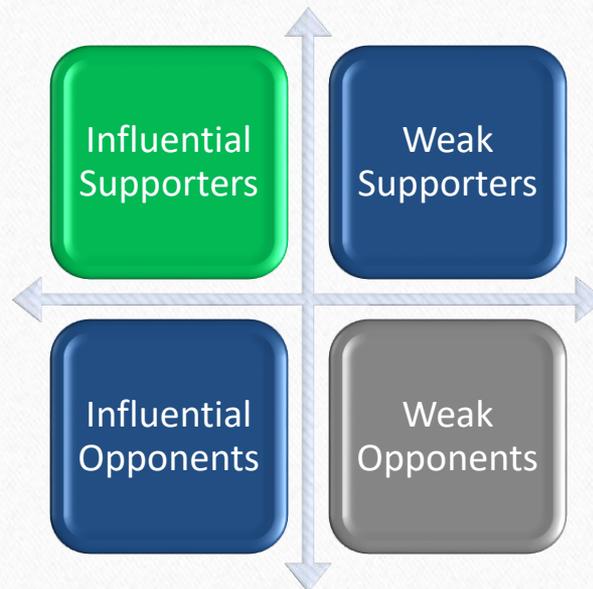
Common Issues

- Missing stakeholders
- Targeting too many stakeholders
- Targeting the wrong stakeholders

Signs of Engagement

- ✓ Responsive and supportive
- ✓ Regular attendance and participation
- ✓ Allocate and provide resources

Segments By Pull and Stance



Use Prioritized Tactics For Each Segment

Recruit, Restrict, Retain, and Reward

Opponents

Recruit and Restrict Influential

Recruit and Retain Weak

Supporters

Retain and Reward

Other approaches

- Use direct communication
- Use steering committee
- Create wins and build successes
- Do the right thing for the enterprise!

Conflict

- Is often inevitable and decreases productivity
- Intensity increases with complexity, despite governance
- Is commonly approached with Win-Lose as first response (*spoiler – this is not a good thing*)

Recommendations

- ✓ Build in conflict resolution processes and use them
- ✓ Use direct approach; avoid conflict avoidance
- ✓ Strive for Win-Win, requires more collaboration vs. compromise

Questions?



Virginia Information Technologies Agency

VITA Security Program

Bill Stewart-VITA

Service Owner, Security Operations

ISOAG Meeting

May 1, 2019



Agenda

- The Transition
- Service Fair
- MSI Model
- Security Capabilities/Services
- Q/A

VITA Service Transition



- **Past** - Single vendor
- **Present** - WITO
Multiple suppliers
legacy toolsets,
services and
processes.
Transitioning to...
- **Future** - Multiple
suppliers, new
technologies/services,
new processes



Changes Coming

- New tool sets being stood up
- Rates being set
- Service Catalog being developed
- Many new services/capabilities after July 1
- To find out more, come to our...

VITA Services Fair



- When
 - Wednesday, May 8, 2019
 - 12:30 - 3 p.m.
- Where
 - CESC multipurpose Rooms
- What
 - Learn about coming services



Review VITA Model-MSI-STC

- MSI
 - Keystone/central spoke for suppliers
 - Cross-functional services
 - VITA's service management portal
- STC - Service Tower Supplier
 - Managed security (MSS)
 - Messaging
 - Mainframe
 - EUS/managed print
 - Voice/network
 - Server/storage/datacenter

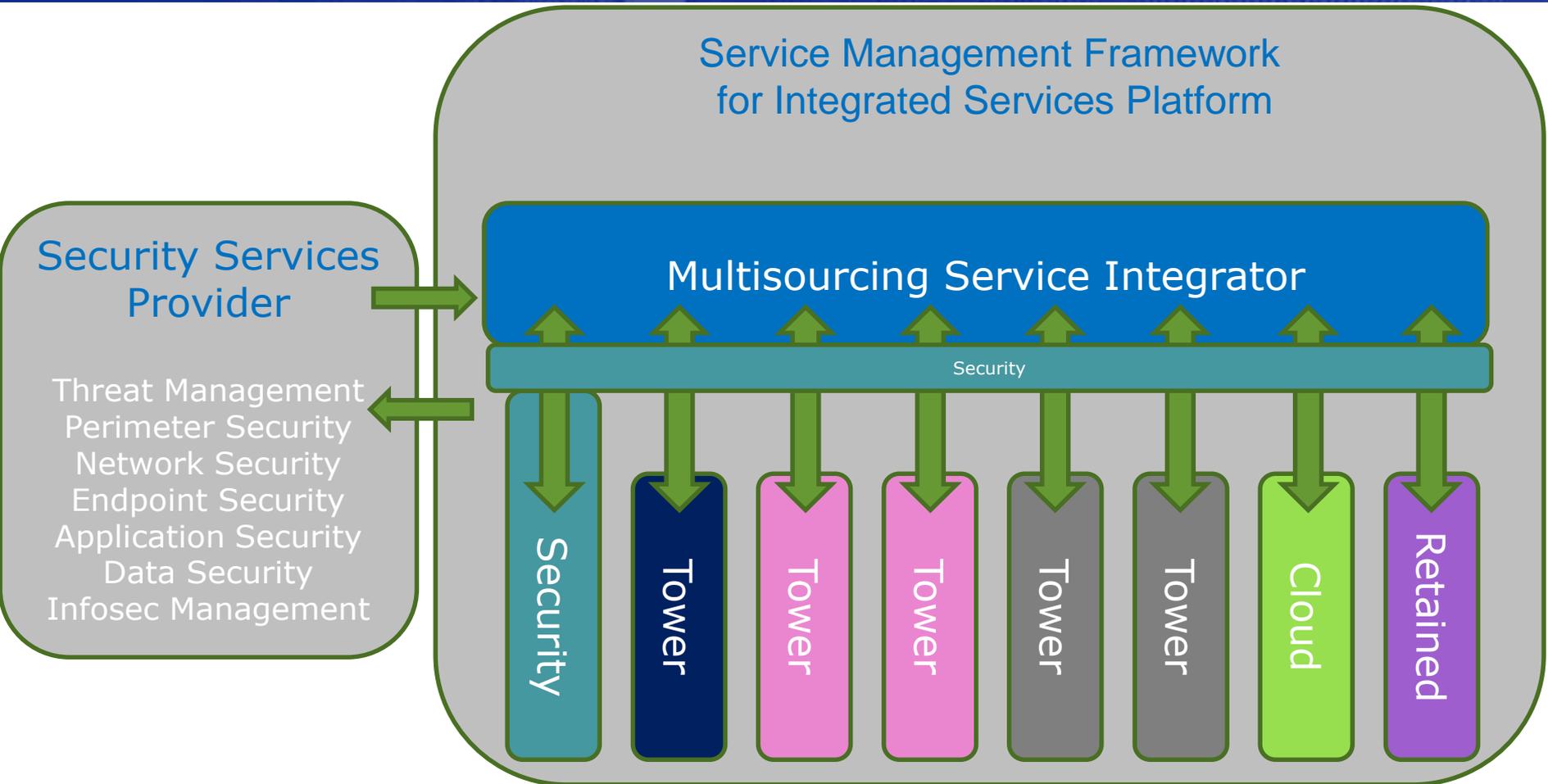


New Security Model

- MSS- will provide services to program STS' and customers
- Example - MSS scan and report vulnerabilities/compliance issues to MSI
 - Each STS responsible to configure and patch their assets
 - STS separation of duties. Difficult to conceal vulnerability/compliance issues.
 - QA/QC through SLA/OLAs
- More services for entities outside of the program (authorized users)



Security Services Delivery





The Players

- MSI - SAIC
- MSS - Atos
- SSSDC - Unisys
- VDN - Verizon
- Messaging - Tempus Nova
- End User Compute - Ironbow
- Managed Print - Xerox
- Mainframe - Perspecta



MSS Scope of Duties

- Notable items NOT in MSS scope
 - Email/SPAM security- (Tempus Nova/Google)
 - Privileged account management (SAIC)
 - Remote access VPN (Unisys)
 - Point to Point tunnels (Verizon)
 - Mainframe ACF2 (Perspecta)
 - Encryption of databases** (Unisys)
 - Database security (Unisys)
 - Volumetric DOS (Verizon)
 - Patching/configuring other STS's



New MSS/STS/Agency Interactions

Platform Tools

- WAF/Server HIPS rulesets
- Network compliance – NAC
- Encryption key management platform
- Certificate management platform
- Vulnerability scans...“fragile systems” (STS, agency)
- Layer 4-7 firewalls

“Optional” items

- Encryption (database, file/folder, etc.)
- DLP/e discovery
- “Legacy services”- firewalls, application whitelisting, etc.



Security Scope: Incidents >> Breaches

- Traditional (incidents)
 - AV/firewalls/IPS/SIEM/Web Security/etc.
 - Baked into VITA services
 - Experience with many current tools - smoother transition
- New capabilities (breaches*)
 - Upper layer firewalls (4 to 7)*
 - WAF*
 - Source code scanning*
 - Privileged account management* (MSI tool)
 - Spam/phishing protection*(messaging tool)
 - DLP*
 - E-discovery "Vault"
 - NAC (part of compliance)
 - Encryption (file-folder/tokenization)
 - Certificate/key management platforms

*Phishing/application layer/privileged accounts- Where most breaches are occurring



Resource Unit Family – Monitoring, Reporting and response

MSS RUs	Definition	Units
Security Incident Management	The management of Security Incidents assigned to the Supplier, including Security Incident response; and the Services necessary to resolve Security Events	Fixed fee
Digital Forensic Investigation	The specialized work that prepares an organization to prosecute for a data breach, theft or loss.	Fixed fee
Response Preparedness	The major Incident (emergency) response process defined as part of the security plan that needs to be exercised every time the plan changes or every other year.	Per response readiness test
Security Monitoring, Log Management, and Analysis	The collection, aggregation and retention of system logs and the monitoring and analysis of that data from connected devices.	Per device monitored



Resource Unit Family - Network and Platform Protection

N-New O-Optional D-Different

MSS RUs	Definition	Units
Desktop Encryption ~N	Portable Devices or Desktops with VITA's required endpoint encryption solution installed and managed by Supplier	per Device
Desktop Managed Host Intrusion Protection, Firewall, & Antivirus	The Desktops monitored by the Supplier using the host based intrusion detection system	per Desktop
Server Encryption -N	Servers in with VITA's required endpoint encryption solution installed and managed by Supplier	per Device
Server Managed Firewall and Antivirus	Managed antivirus (Malware Protection) and Firewall solution, provided by Supplier for Servers	per Server
Server Managed Host Intrusion Protection	Managed services provided to servers monitored by the Supplier using the host based intrusion detection system	per Server
Managed Network Intrusion Protection	Services managed by Supplier and used to provide Managed Network Intrusion Protection (100 MB / 1 GB / 10 GB of effective throughput)	per Unit
Data Loss Prevention -N, O	End users utilizing the Supplier provided Data Loss Prevention service	per User
Web Content Monitoring	Monitoring and filtering by a device that is connected to the VITA Network by the Supplier to monitor and filter content (650 Mbps / 1350 Mbps/ 4200 Mbps of effective throughput)	per Unit



Resource Unit Family - Network and Platform Protection - Continued

N-New O-Optional D-Different

MSS RUs	Definition	Units
Managed Firewall -D	Managed traffic inspected by a firewall device managed (blocked or not) and include the firewall hardware, software, design, installation, maintenance and management (100 MB / 1 GB / 10 GB)	per Unit
Vulnerability Scanning -D	Active IP addresses scanned as part of a regular or scheduled scan of the environment to detect vulnerabilities	IP Addresses
Application Scanning -N, D	Scanning of website URLs to detect vulnerabilities (exposed to the internet or restricted to internal segments)	per URL
Penetration Testing	Regular or scheduled scanning of website URLs to detect vulnerabilities (exposed to the internet or restricted to internal segments)	Fixed Fee
Compliance Testing -N, D	Aggregate number of network or endpoint devices receiving compliance testing	per Device
Application Process Whitelisting -N, O	Devices receiving Application Process Whitelisting and Endpoint File Integrity Checks	per Device



Resource Unit Family- Network and Platform Protection - 3

N-New O-Optional D-Different

MSS RUs	Definition	Units
Full Packet Capture	Amount of Full Packet Capture services for Legacy systems, DC appliances, 44TB storage and remote appliances)	Fixed Fee
WAF -N, O	Amount of Web Application Firewalls managed by Supplier for low, medium and high capacity consumption, as well as legacy and cloud instances	per Unit
File Level Encryption -N, O	Users receiving File Encryption Services	per User
e-Discovery -N, O	Devices receiving e-Discovery Services	per Device
Tokenization License -N, O	Annual license subscriptions utilized for Tokenization	per Annual License
Managed Encryption Platform -N, D	Up to 1,000,000 maximum keys and/or 1,000 concurrent connections	Fixed Fee
Encryption License -N, O, D	Annual license subscriptions utilized for Encryption services as part of the Managed Encryption Platform Service, including: File protection, application layer encryption, database native, KMIP connector, VM encryption, database encryption	per Annual License
Source Code Scanning -N, O	Annual subscriptions utilized for Source Code Scanning, including 7 types of licenses	per Annual License



Resource Unit Family- Network and Platform Protection - 4

N-New O-Optional D-Different

MSS RUs	Definition	Units
Certification Management Solution -N, O	Aggregate number of server or end user devices receiving Certificate / Key Management services	per Server Device
Managed Virtual Firewall -N, O	Firewalls managed in the virtual environment (5 types)	per Unit
Sandbox -N	Annual License Subscriptions utilized for enhanced security capabilities for the physical 10GB and 1GB firewalls	per Annual License
Firewall Self-Service Platform -N, O	Additional firewall capabilities for user reporting, change management automation, application performance metrics	Fixed Fee
Topology/Firewall Workflow -N, O	Annual License Subscriptions utilized for Firewall Self-Service Platform Services elements	per Annual License
Business Connectivity Visualizer- N, O	Annual License Subscriptions utilized for Firewall Self-Service Platform Services elements	per Annual License
Cloud Access Security Broker (CASB) -N, O	Aggregate number of End Users receiving Cloud Access Security Broker service	per User



Questions?

Contact info:

Bill Stewart

bill.stewart@vita.virginia.gov

Managed security contract documents link:

<https://www.vita.virginia.gov/services/it-infrastructure-services/>



Virginia Information Technologies Agency

Upcoming Events





Future ISOAG

June 5, 2019 @ CESC 1 – 4 p.m.

Speakers: Benjamin Gilbert, DHS
Kathy Bortle, VITA
Darrell Raymond, ATOS

ISOAG meets the first Wednesday of each month in 2019

Adjourn

Thank you for attending

