PRICE®

COST ESTIMATION SOLUTIONS

Estimate with Confidence™

Ownership Cost of Cybersecurity in Cloud Based IT Systems



Richard Mabe, Solutions Consultant

26 September 2018

Foreword

Life cycle cybersecurity protection of information technology (IT) systems has become a critical issue

- Internet of Things
- Aggressive nature of Cyber attacks

Users need to evaluate and compare most effective approach for cybersecurity protection with the life cycle cost (TOC) to host and operate IT systems

- Cloud
- User owned data center

This paper presents a business case framework to evaluate TOC and cybersecurity trade-offs

Additional Contributors:

- Zachary Jasnoff; VP Professional Services, Price Systems LLC
- Davis Cass; VP Cloud Global Security Services; IBM

Overview

Scope and Definition of IT

Cloud Based Services/Support

Cloud Cybersecurity Concerns

Cybersecurity Total Ownership Costs

Evaluating Cost Trade-offs

Scope and Definition of IT

Assess for DOD System Integration → Authority to Operate on DOD Networks

Communications Information Mgmt Radar, Navigation

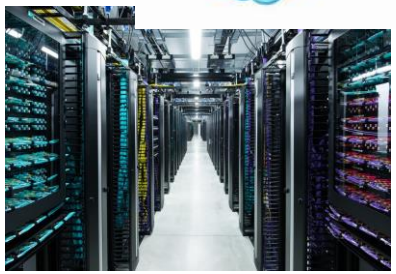
Data management Intelligence Control/Monitor

IT Products and Services (IOT)

Integrated To Be

Platform IT

Information Systems and Enclaves

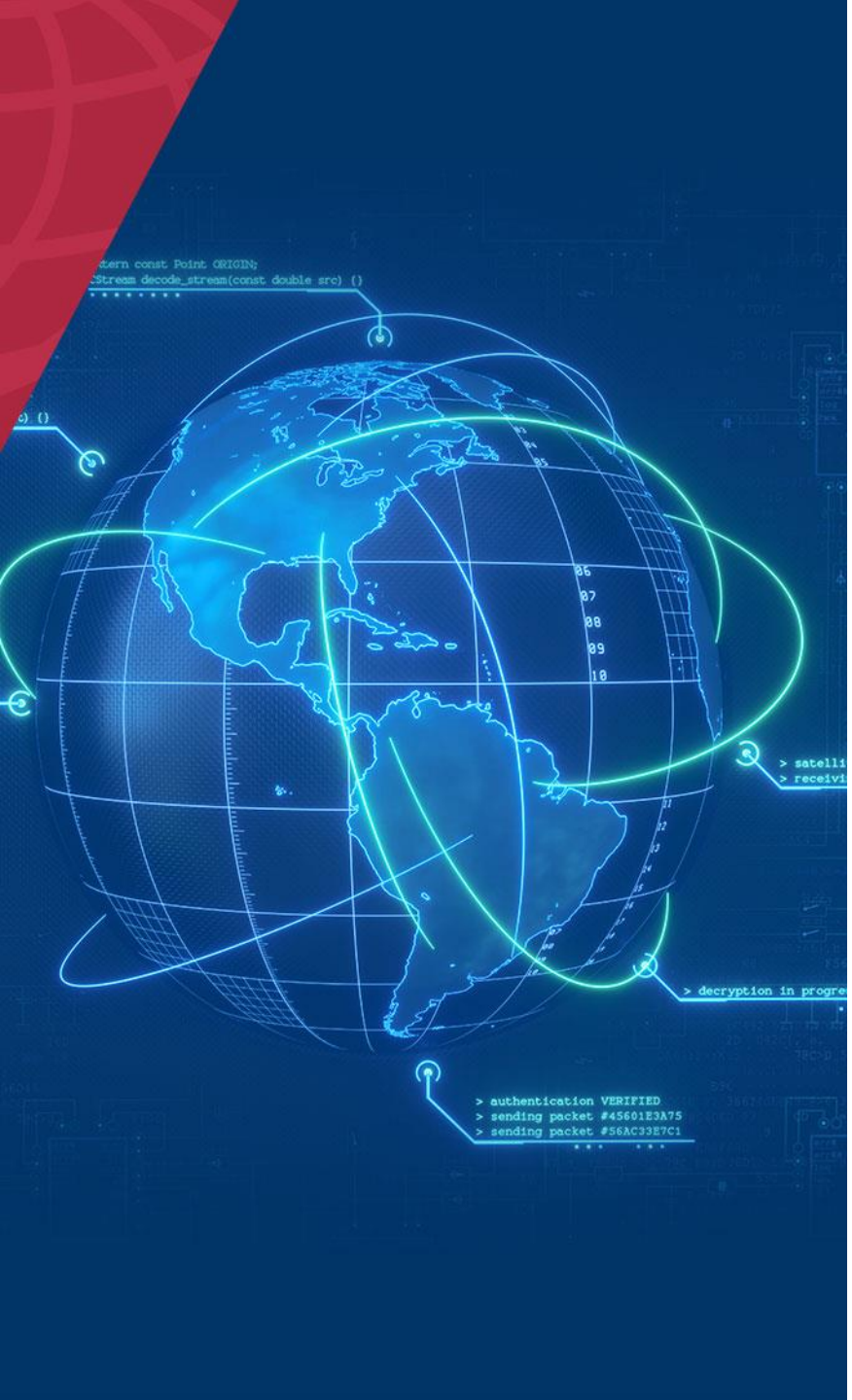


IT System Cybersecurity Functions

Cybersecurity capability within a system: Products, Services (HW and SW)

Cybersecurity as the primary mission function of an IT system:

- Offensive/Defensive
- Test and Evaluation
- Vulnerability Assessment/Hunter
- Cyber Command and Control



Cloud Based Services and Support

Cloud is a means to an end, enabling many benefits …

Faster to market	Higher Quality	↓Cost ↑ Flexibility	Repeatable & Scalable	Secure & Compliant
Enable experimentation *Fail or succeed fast* *Accelerated releases* *Rapidly add capacity*	*Frequent user feedback* *Fewer errors* *Analytics based decisions* *Resiliency thru automation*	*Transparent / variable structure* *Affordable infrastructure* *Service provider choice* *Address technical debt*	*Standardization (No Snowflakes)* *Reference implementations* *Skill acquisition/upgrade* *Expansion consistency*	*Fewer audit exceptions* *Regulatory requirements* *Process control structures* *Client confidence*

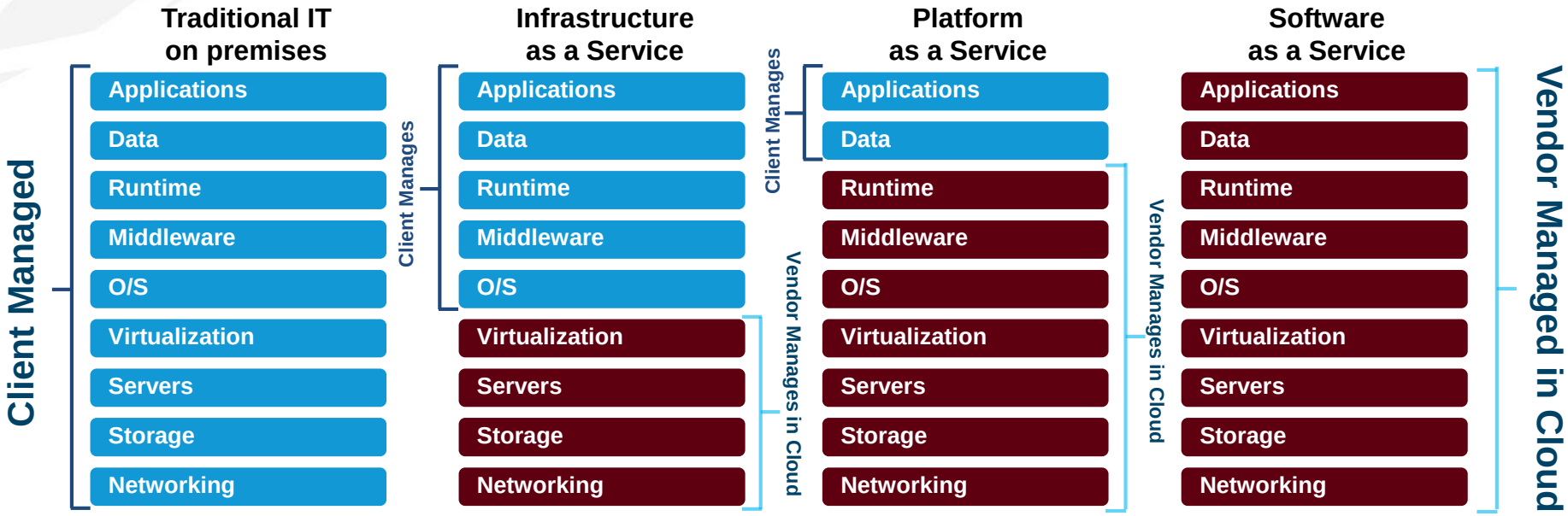
… that require organizations to transform, and re-think –

- *How to deliver IT capabilities while improving quality*
- *How to interact and react with clients*
- *How to resolve technical debt*
- *How to meet cybersecurity requirements and mitigate cybersecurity threats*

Cloud Business value is driven by Workload -

- Best Fit: Info Mgmt, Data Mgmt, C4I Apps

Service Delivery Models



Integration of Roles, Processes, Information, and Technology requires additional cloud service management

Additional Service Management Needed

Provided by Cloud Provider

Cloud Cybersecurity Concerns

Management Concerns

What Holds us Back

Privacy and Compliance Issues

- Adapting to a risk-based approach (RMF)

Insider Threats

- Cloud host employees, contractors, partners

Cloud Host Skills Gap

- 209,000 cybersecurity jobs in the U.S. are unfilled
- Postings are up 74% over the past five years

Innovation

- CISCO estimates that by 2020 there'll be 50 billion devices connected to the IOT

Advanced Attacks

- More than 80% involve cyber gangs, a global business that accounts for $400B+ a year

The Solution: A Well Planned Transition

As Is System

(User Data Cntr)

- Operate
- Sustain

Recurring Costs:

- Labor
- Materials
- Overhead
- ODCs
- Facilities
- PM/SE

Plan for Transition:

- *Business Case*
- *Change Mgmt*
- *Svc Level Agreement*

- What
- When
- Where To
- Security
- Access

Transition:

- Software
- Data
- Interfaces

Non-Recurring Costs:

- Modify/Refactor SW apps
- Prep data for migration
- Develop new middleware Interfaces
- Adapt to Cloud OS and Middleware Services
- PM/SE

Execute Plan:

- *SW Porting*
- *Data Migration*
- *User Training*

- Migrate
- Instantiate
- Test/Verify
- Parallel Ops
- Changeover
- Go Live

To Be System

(Cloud Host)

- IaaS
- PaaS
- SaaS

Recurring Costs:

- Fees
- Licenses
- Subscriptions

For:

- Infrastructure
- Run Time Env
- SW Services
- Access
- Cybersecurity
- PM/SE

Cybersecurity Planning

Phase 1: Project Initiation:

- Collect and review data; prepare transition team and assets

Phase 2: Assess the As Is Security Posture

- Catalog current cloud use; prepare assessment report for the client

Phase 3: Define the “target” To Be state

- Analyze Requirements for the To Be Domain (Gap Analysis); present cloud security maturity framework

Phase 4: Recommend a Cloud Solution Roadmap

- And (potentially) a Business Case for the level of Cloud service

Cybersecurity Approach

Cloud Security & Regulatory Compliance Accelerators:

- Assess the maturity and effectiveness of the current security program in-place at the client's organization
- Manage and govern information security more effectively and efficiently at all levels of the Cloud stack
- Identify and effectively manage security and regulatory compliance requirements while driving growth of programs
- Build a more risk aware culture through education and awareness
- Improve operational security for critical infrastructure

Cybersecurity Policies

Cooperative effort (user/host)

- Identify, evaluate, implement and enforce security policies aligned to the delivery model: IaaS, PaaS, SaaS

Cloud service consumers and cloud service providers

- Establish and follow their respective cloud security policies

User's cloud-specific security policies

- Likely reflect their corporate security policies

Cybersecurity Total Ownership Costs

TOC Scope for Cloud Apps

Measures all costs over the system's life cycle

TCO = Capital Expenses + Operational Expenses + IT Governance/Sys Mgmt

(Direct)	(Direct + Indirect)	(Overhead/Admin)
(Infrastructure)	(Services)	(PM, FM, SE, Cyber Mgmt)

Budget focus

- Changes from CAPEx to OPEx during and after transition

Cost Impacts for the System Owner:

- Changes the acquisition model: infrastructure not procured
- Changes the compliance / security model: Cloud security svcs
- Changes the management model: Cloud provider systems mgmt

Cost Elements for Cybersecurity

Cost Elements
Mil-Std-881D
Cybersecurity Focus

Business System - Cyber Specific LCC
Capital Expenses
Cybersecurity Integration - Governance and Org
Custom Workload
Cybersecurity Services (SW)
Cyber End User Device (HW)
Cyber Data
System Level Technology
Dedicated Cyber Comm
Infrastructure Services
Systems Engineering (RMF)
Cyber Test and Evaluation
Operations Expenses
Cybersecurity Services - Governance and Org
System/Services Operations
Cybersecurity Services
Cyber Data Services
End User Device Support Services
Training Services Operations
System/Services Mgmt
Communications Services
Infrastructure Services
Cyber SW Maintenance/Modification
Managed Services Operations
Systems Engineering (RMF)
Recurring Cyber Tests

- **Organized with Mil-Std-881D WBS, App J**
  - Highlights Cybersecurity costs for trade-off
  - analysis
  - Includes Operating and Support costs

- **Cybersecurity costs do not all carry equal weight**
- **Drivers include:**
  - Systems Engineering Labor (Initial RMF)
  - Support Engineering Labor (Recurring RMF)
  - Initial and Recurring Cybersecurity Tests
  - Life Cycle Risk Management
    - *High replacement rate for vulnerable SW/HW*
    - *Continuous monitoring and threat analysis*
    - *Continuous validation of controls related to confidentiality, availability and integrity requirements*

Map to Complete WBS- Development

Cost WBS (Mil-Std-881D, App J) →

Cybersecurity CES ↓

	1 Business System	1.1 Development/Procurement	1.1.1 Custom Application Development	1.1.1.1 Enterprise Services Elements	1.1.1.4 System Level Hardware	1.1.2 System Level Integration	1.1.3 Systems Engineering	1.1.3.1 Cyber Systems Engineering	1.1.4 Program Management	1.1.4.1 Cyber Program Management	1.1.5 Change Management	1.1.6 Data Management	1.1.7 System Test and Evaluation	1.1.7.1 Cybersecurity Test and Evaluation	1.1.12 Operational Site Infrastructure	1.1.12.1 Hardware	1.1.12.2 Software Licenses
Business System - Cyber Specific LCC				X	X	X		X		X	X	X		X	X	X	
Capital Expenses																	
Cybersecurity Integration - Governance and Org										X	X						
Custom Workload																	
Cybersecurity Services (SW)				X													X
Cyber End User Device (HW)					X												
Cyber Data												X					
System Level Technology																	
Dedicated Cyber Comm																X	
Infrastructure Services															X		
Systems Engineering (RMF)						X		X									
Cyber Test and Evaluation														X			

Map to Complete WBS- Sustainment

Cost WBS (Mil-Std-881D, App J) →

Cybersecurity CES ↓

	1 Business System	1.2 Recurring Annual Business System Sustainment	1.2.1 Program Management	1.2.2 Systems/Sustainment Engineering	1.2.3 Change Management	1.2.4 Help Desk	1.2.5 Data Cleansing/Data Mgmt	1.2.6 System Data Base Admin	1.2.7 IT Infrastructure/Network Maintenance	1.2.7.3 Management	1.2.8 HW Tech Refresh	1.2.8.1 Cybersecurity Equipment	1.2.9 SW Licenses Refresh/Update	1.2.9.1 Cybersecurity SW License	1.2.10 Cybersecurity Maintenance Management	1.2.10.1 Compliane Operations and Tracking (RMF)	1.2.10.2 FOTE	1.2.10.3 Certification/Validation	1.2.11 Follow On User Training	1.2.13.2 Software (Includes Cybersecurity and IAVA)
Operations Expenses																				
Cybersecurity Services - Governance and Org																				
System/Services Operations			X		X	X														
Cybersecurity Services														X						
Cyber Data Services							X	X												
End User Device Support Services												X								
Training Services Operations																			X	
System/Services Mgmt																				
Communications Services																				
Infrastructure Services										X										
Cyber SW Maintenace/Modification																				
Managed Services Operations																				X
Systems Engineering (RMF)				X												X		X		
Recurring Cyber Tests																	X			

Evaluating Cost Trade-offs

Trade-Offs for IaaS:

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

Transition

To Be: IaaS
Fee for Svc
Virtual Domain

Business System - Cyber Specific LCC	As Is Total Cost of Ownership	To Be Total Cost of Ownership (IaaS)
Capital Expenses		(Basic Infrastructure)
Cybersecurity Integration - Governance and Org	User Funded Program Mgmt (Governance)	
Custom Workload	Workload	
Cybersecurity Services (SW)	User Owned/Managed App SW	
Cyber End User Device (HW)	User Owned/Managed App HW	
Cyber Data	User Owned Data Services	Fee for Cloud Provided Data Storage
System Level Technology	Technology	
Dedicated Cyber Comm	User Owned/Managed Comm	
Infrastructure Services	User Owned/Managed Infrastructure	Fee for Cloud Virtual Domain Services
Systems Engineering (RMF)	User Funded Systems Engineering	
Cyber Test and Evaluation	User Funded Systems Test/Eval	
Operations Expenses		(Basic Infrastructure)
Cybersecurity Services - Governance and Org	User Funded Program Mgmt (Governance)	
System/Services Operations	Workload Management and Operations	
Cybersecurity Services	Data Center/Corporate Staff	
Cyber Data Services	Data Center/Corporate Staff	Fee for Recurring Cloud Data Storage/Management
End User Device Support Services	Data Center/Corporate Staff	
Training Services Operations	Data Center/Corporate Staff	
System/Services Mgmt	Technology Management and Operations	
Communications Services	Data Center/Corporate Staff	
Infrastructure Services	Data Center/Corporate Staff	Fee for Recurring Cloud Provided/Managed Infr Services
Cyber SW Maintenance/Modification	SW Maintenance and Modifications	
Managed Services Operations	User Owned/Managed SW Services	Fees for Recurring Cloud Managed Help Desk/User Services
Systems Engineering (RMF)	User Funded RMF for Apps/Data	Fees for Recurring Cloud Provided Infrastructure Service
Recurring Cyber Tests	User Funded RMF for Apps/Data	Fees for Recurring Cloud Provided Infrastructure Service

Trade-Offs for PaaS:

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

→ Transition →

To Be: PaaS
Fee for Svc
Virtual Domain

Business System - Cyber Specific LCC	As Is Total Cost of Ownership	To Be Total Cost of Ownership (PaaS)
Capital Expenses		(Add Platform Services)
Cybersecurity Integration - Governance and Org	User Funded Program Mgmt (Governance)	
Custom Workload	Workload	
Cybersecurity Services (SW)	User Owned/Managed App SW	
Cyber End User Device (HW)	User Owned/Managed App HW	Cloud Provided Run Time Services (License/Fees)
Cyber Data	User Owned Data Services	Fee for Cloud Provided Data Storage
System Level Technology	Technology	
Dedicated Cyber Comm	User Owned/Managed Comm	Cloud Provided/Managed Platform Services (License/Fees)
Infrastructure Services	User Owned/Managed Infrastructure	Fee for Cloud Provided Virtual Platform Service
Systems Engineering (RMF)	User Funded RMF for Apps/Data	Cloud Provided/Managed PlatformServices (License/Fees)
Cyber Test and Evaluation	User Funded RMF for Apps/Data	Cloud Provided/Managed Platform Services (License/Fees)
Operations Expenses		(Add Platform Services)
Cybersecurity Services - Governance and Org	User Funded Program Mgmt (Governance)	
System/Services Operations	Workload Management and Operations	
Cybersecurity Services	Data Center/Corporate Staff	Fee/License for Recurring Cloud Cyber Services
Cyber Data Services	Data Center/Corporate Staff	Fee for Recurring Cloud Data Storage/Management
End User Device Support Services	Data Center/Corporate Staff	Fee/License for Recurring Cloud Platform Mgmt and Ops
Training Services Operations	Data Center/Corporate Staff	Fee/License for Recurring Cloud Platform Training Svcs
System/Services Mgmt	Technology Management and Operations	
Communications Services	Data Center/Corporate Staff	Fee/License for Recurring Cloud Provided/Managed Comm Svcs
Infrastructure Services	Data Center/Corporate Staff	Fees for Recurring Cloud Provided/Managed Infr Services
Cyber SW Maintenace/Modification	SW Maintenance and Modifications	
Managed Services Operations	User Owned/Managed SW Services	Fee for Recurring Cloud Managed Help Desk/User Services
Systems Engineering (RMF)	User Funded RMF for Apps/Data	Fee/License for Recurring Cloud Provided Platform Service
Recurring Cyber Tests	User Funded RMF for Apps/Data	Fee/License for Recurring Cloud Provided Platform Service

Trade-Offs for SaaS:

Cost Elements
Mil-Std-881D
Cybersecurity Focus

As Is: Data Center
User Owned
Vertical Integration

→ Transition →

To Be: SaaS
Fee for Svc
Virtual Domain

Business System - Cyber Specific LCC	As Is Total Cost of Ownership	To Be Total Cost of Ownership (SaaS)
Capital Expenses		(Add Cloud SW and SW Services)
Cybersecurity Integration - Governance and Org	User Funded Program Mgmt (Governance)	Cloud Provided Program Mgmt (Governance)
Custom Workload	Workload	
Cybersecurity Services (SW)	User Owned/Managed App SW	Cloud Provided Application SW (License/Fee)
Cyber End User Device (HW)	User Owned/Managed App HW	Cloud Provided Run Time Services (License/Fees)
Cyber Data	User Owned Data Services	Fee for Cloud Provided Data Storage
System Level Technology	Technology	
Dedicated Cyber Comm	User Owned/Managed Comm	Cloud Provided/Managed Platform Services (License/Fees)
Infrastructure Services	User Owned/Managed Infrastructure	Fee for Cloud Provided Virtual Capability
Systems Engineering (RMF)	User Funded Systems Engineering	Cloud Provided Service for Platform HW/App SW (License/Fee)
Cyber Test and Evaluation	User Funded Systems Test/Eval	Cloud Provided Service for Platform HW/App SW (License/Fee)
Operations Expenses		(Add Cloud SW and SW Services)
Cybersecurity Services - Governance and Org	User Funded Program Mgmt (Governance)	Cloud Provided Program Mgmt (Governance)
System/Services Operations	Workload Management and Operations	
Cybersecurity Services	Data Center/Corporate Staff	Fee/License for Recurring Cloud HW/SW Cyber Services
Cyber Data Services	Data Center/Corporate Staff	Fee for Recurring Cloud Data Storage/Management
End User Device Support Services	Data Center/Corporate Staff	Fee/License for Recurring Cloud Platform Mgmt and Ops
Training Services Operations	Data Center/Corporate Staff	Fee/License for Recurring Cloud Platform Training Svcs
System/Services Mgmt	Technology Management and Operations	
Communications Services	Data Center/Corporate Staff	Fee/License for Recurring Cloud Provided/Managed Comm Svcs
Infrastructure Services	Data Center/Corporate Staff	Fees for Recurring Cloud Provided/Managed Infr Services
Cyber SW Maintenace/Modification	SW Maintenance and Modifications	
Managed Services Operations	User Owned/Managed SW Services	Fee/License for Recurring Cloud Managed Help Desk/User Svcs
Systems Engineering (RMF)	User Funded Systems Engineering	Fee/License for Recurring Cloud Provided Platform Service
Recurring Cyber Tests	User Funded Systems Test/Eval	Fee/License for Recurring Cloud Provided Platform Service

Evaluating Trade-offs

Measure cloud performance in context of workload

- Not just price, but Price-Performance that matters (band for buck)

What to consider:

- Real requirements (capabilities) for Apps, Workload, Security, Service

  Can the provider meet requirements for Confidentiality, Availability and Integrity?

- Performance in the cloud; including: flexibility to position workload; access to emerging technology; scalability

  Are secure, high speed choices available for sensitive workloads?

- Economics; including: choice of technologies; visibility and control of user resources; ability to optimize ROI

  What is the current and future cost of Security-Performance? Are there hidden costs?

**Cloud IT Economics, What you don't know about TCO can hurt you. IBM Corp., 2018*

Compare Meaningful Measures

Measures to consider for Cloud applications:

- Web response: bandwidth/process speeds; ability to expand quickly

  Can the provider meet requirements for cybersecurity controls?

- Data storage/retrieval: I/O queries per hour; unit cost of storage

  Is secure storage readily available and accessible at an affordable rate?

- Inter-networking capability: cloud-to-cloud; cloud-to-data center; data center-to-data center (edge computing)

  What is the cost of security for a messaging intensive workload?

- Cloud host: speed and efficiency of SW porting and Data migrations to the cloud for highly secure applications

  How efficiently does the provider move data and workloads?

Trade-off Methodologies:

Example 1: The Cloud Price Index (cPCI)*

- Required Labor for VM Support vs VM Utilization and Capacity
- Derive average price of a cloud solution using “basket of goods” approach:

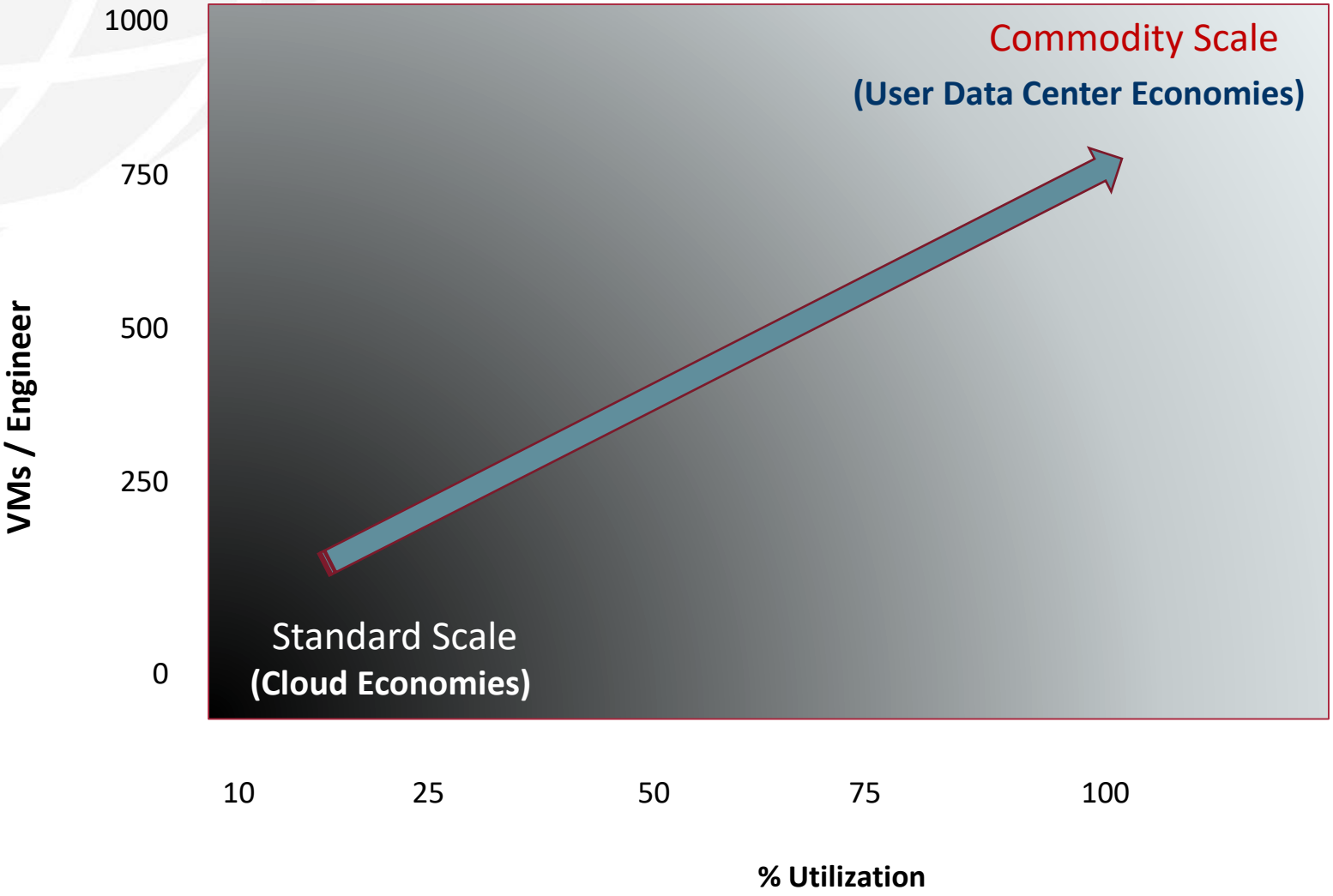
  Determine the total cost of a bundle of services (IaaS, PaaS, SaaS)

  Estimate the average “Cost for VM Hour” and “Price per GB month”
- Compare and evaluate options based on Labor Efficiency and VM Use:

  The more VMs a single administrator/system engineer can manage, the lower the unit “Cost per VM Hour”

  The more Capacity Use per VM, the lower the “Cost per GB Month”

** Total cost of ownership in private cloud: guidelines for buyers. O. Rogers and J. Atelsek, 451 Research, Sept 2017*



Trade-off Methodologies:

Example 2: Predictive Analytics

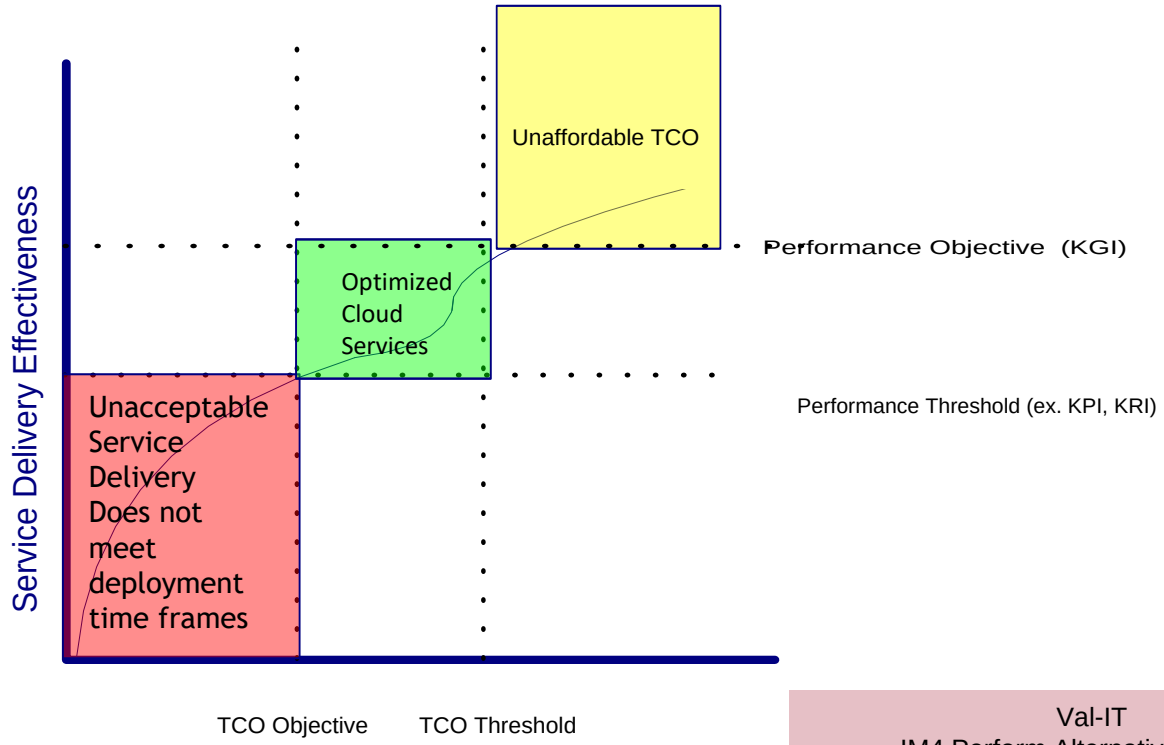
- Employ a wide variety of statistical techniques, such as modeling, machine learning, and data mining to rapidly analyze current and historical facts to predict future (unknown) events/outcomes
- Apply to Cloud Workloads; consider framework tools:
  - Consider control requirements, technical issues and business risks to minimize service interruptions / optimize continuous service (Tool: Control Objects for Information and Related Technology – CobIT)
  - Consider also IT System Governance and Business Investments to minimize life cycle cost and optimize budget performance (Tool: Value from IT Investments – VAL IT
- Best practice: extend CAIV framework to cloud workloads (Objectives, Thresholds)

Evaluate Investment Performance and System Delivery Effectiveness:

CobiT DS4 Ensure Continuous Service

Ensure that IT service and infrastructure can resist and

recover from failures…



Typical KPI

- Time to Market
- Patching (IAVA)
- SLA

Val-IT
IM4 Perform Alternative Analysis
IM7 Identify Full Life Cycle Costs and Benefits

Control Objects for Information and Related Technologies
+Value from IT Investments

The Optimized TCO provides the essential "best value" framework for the strategic decision process

Wrap-up

Cybersecurity related costs are included in a number of places in a system TCO Cost Element Structure: HW, SW, Infrastructure, Governance, Operations / Sustainment / Modifications

Cost drivers are likely Labor costs for Systems Engineering labor and Test events supporting Risk Based Management of Cybersecurity requirements for the system's life cycle

The optimal TCO solution is likely an affordable mix of user owned and managed applications that employ Cloud Infrastructure and Virtual Platforms

- The User maintains responsibility for the Application Cybersecurity Assessment
- The Cloud provider accepts responsibility and maintains authority for their Infrastructure and Virtual Domains/Platforms

Use of predictive analytics, combined with modeling approaches like CobiT, VAL-IT and pCPI provides a consistent framework to holistically and consistently calculate TCO on a lifecycle basis

The process is a life cycle team effort supported by the User and by the Cloud Provider

Richard D. Mabe
Solutions Consultant; Price Systems, LLC

Contact:
(856) 651-8567
richard.mabe@pricesystems.com

Mr. Mabe is a Senior Solutions Consultant within the Services Group of Price Systems, LLC. In this role, Mr. Mabe conducts research and develops modeling tools for a variety of programs within the federal government. Mr. Mabe also helps True Planning users develop custom solutions for life cycle cost estimates and other cost analysis products.

Mr. Mabe has over 40 years of experience as an operations analyst, focusing on logistics analysis and cost estimating for the Air Force and other government programs. Prior to his current position with Price Systems, LLC, Mr. Mabe was a Business Area Manager for Quantech Systems, Inc. at Hanscom AFB, managing a team of 20 analysts developing cost estimating products for Air Force C4I, Cyber and Networking system programs. Prior to his work at Quantech, Mr. Mabe was the Technical Advisor for the IT and Electronics Systems Division of the Air Force Cost Analysis Agency (AFCAA), providing cost research, databases and tailored tools to support independent cost estimates of AF acquisition programs. Mr. Mabe also supported several AF and DOD working groups focused on methods to apply industry best practices for SW development, cybersecurity and C4I systems integration to DOD programs.

Prior to working for AFCAA, Mr. Mabe provided cost estimating and cost analysis support to multiple C4I, Cyber and Networking programs at Hanscom AFB, MA, - for 2 years as a PEO level Cost Chief, and for 13 years as a Technical Expert for Tecolote Research, Inc. Many of these were Joint Service programs, sharing systems and equipment with Army and Navy C4I programs. Prior to working at Tecolote, Mr. Mabe spent 6 years with TASC in Reading, MA managing a team of systems engineers and logistics analysts developing readiness based supply and logistics models for the Air Force. Prior to TASC, Mr. Mabe was an Air Force supply and logistics officer, providing hands-on support to Air Force operations in the CONUS and in USAFE. He completed his active Air Force duties by serving as an Assistant Professor for Inventory Management at the Air Force Institute of Technology.

Mr. Mabe holds a BS Degree in Geology from Boise State University, and an MS in Logistics Management from AFIT. He received a Level 3 DAWIA certification in Business-Cost Estimating, and also a Level 3 DOD Financial Management certification in Cost. He is a recipient of the AF Outstanding Civilian Career Service Award.

