Cybersecurity Cost Issues Facing Today's Cost Analyst

GALORATH

Dan Galorath, CEO, +1 (310) 414-3222 x 614 (PST), galorath@galorath.com
Bob Hunt, President Galorath Federal, +1 (703)201-0651 (EST) Bhunt@Galorath.com

Three Key National Security Initiatives

Space Dominance

Data Analytics/Data Science

Cybersecurity

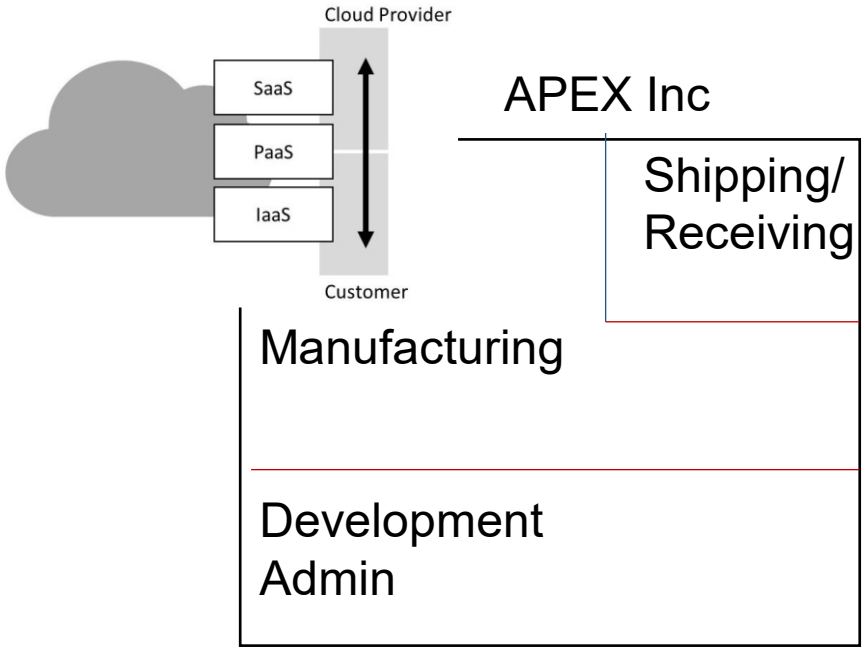
- Army now says Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance and Reconnaissance Center — (**C5ISR)**
- Cloud - Fog – Mist Computing/Costing expands the challenge
- As the Vinn Diagram shows, Cyber is critical to all three areas

Cybersecurity Is Nothing To Worry About “NOT”

A Cybersecurity Example

100'X100' Secure Facility with in-house and cloud applications

APEX Inc is a COCO developing software and integrating it into chips for a classified DoD communications project.



ISSUE 1: How broad is the definition? Does it include (**Cyber-Physical Systems**):

- Building the SCIF, providing perimeter protection, remote monitoring, access control, …?
- Protecting access to the Program Control System (PCS) as well…HVAC, power source, monitoring system etc.?
- Does it include cloud security?
- More than internal network control/monitoring?
- The O&S/sustainment tail
- Disaster recovery plan, Live recovery, Contingency plan, Best practices for recovery

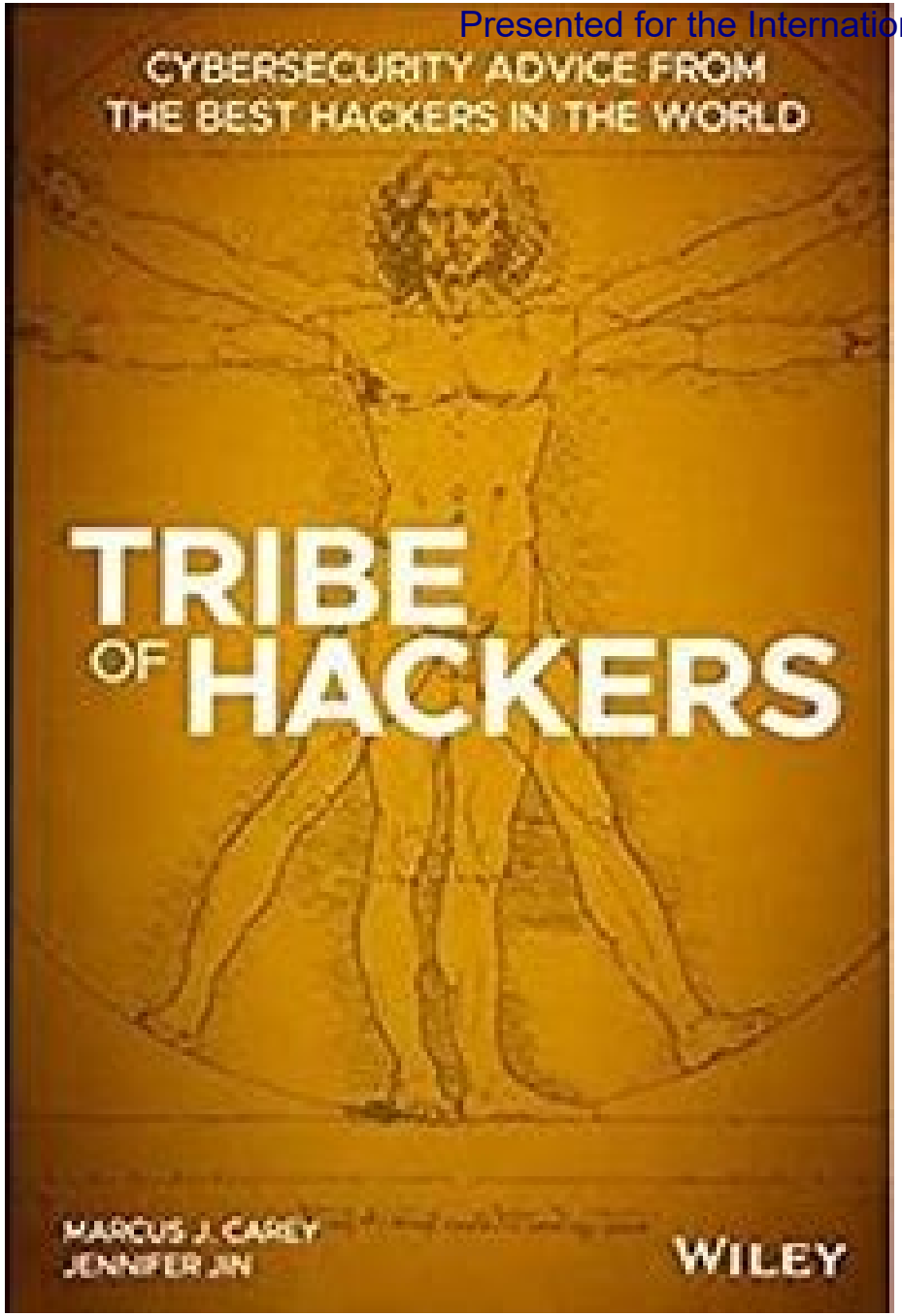
ISSUE 2: Where are the data?

The Big Question: How much should APEX send/the DoD allocate for Cybersecurity?

Some Infrastructure Factors

Source is RS Means 2020

- SCIF space (PAX Newsletter 2020 FAC Code 14162), for a CONUS site, costs $564/SF based on 4,100 SF average size (FY19$).
- A typical Visitor Control Center is $408/SF (FY19$) based on a 2,960 SF space.
- A Gatehouse averaging 933 SF is $731/SF (FY19$).
- Camera & monitor are $1,325 with an adder of $2,300 for pan tilt zoom for a total of $4,625 (FY19$)
- If this is a stand-alone facility you would also want to consider security fencing & AT/FP measures such as bollards.
- If you needed fencing it would be $44.50/LF for an 8’ high security/retention fence (PAX Newsletter 2020 FAC Code 87210)
- Bollards would run $1,351 per (PAX Newsletter 2020 FAC Code 88040)

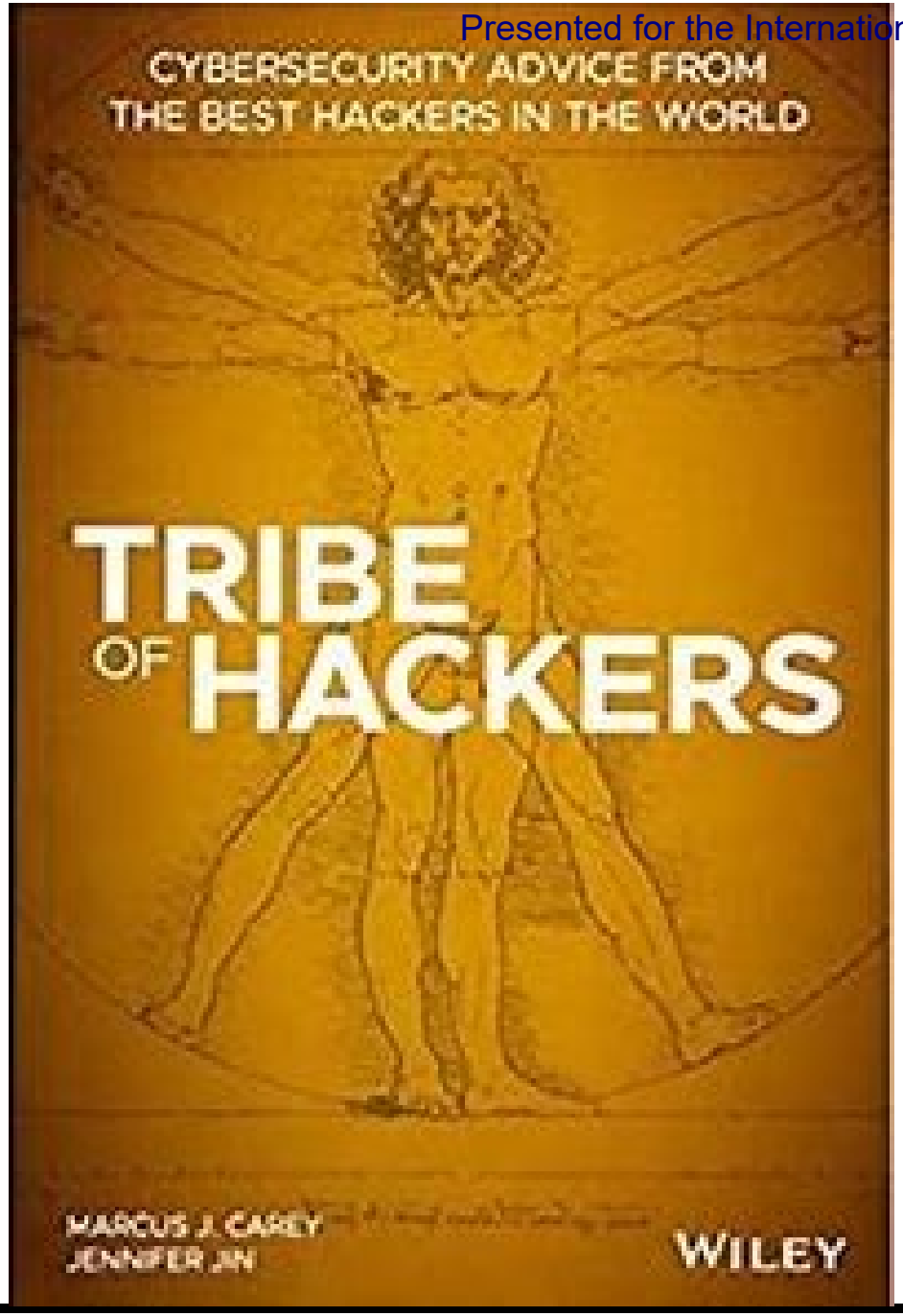


Recommended Reading
The Biggest Myth

"The biggest myth is that we are one technical solution away from solving all of the industry's problems."

"Perhaps I'm just jaded by all the marketing, but I think the biggest myth in security is that risk can be reduced, and security posture can be improved, by purchasing products."

"It's not always the hacker in the black hoodie trying to steal your data, and it's not always about someone trying to steal your personal information, credit card numbers, or secrets. Sometimes, it's the teammate who is still getting their feet wet—but has administrative access to all your systems—who accidentally took down or deleted an entire piece of your infrastructure."

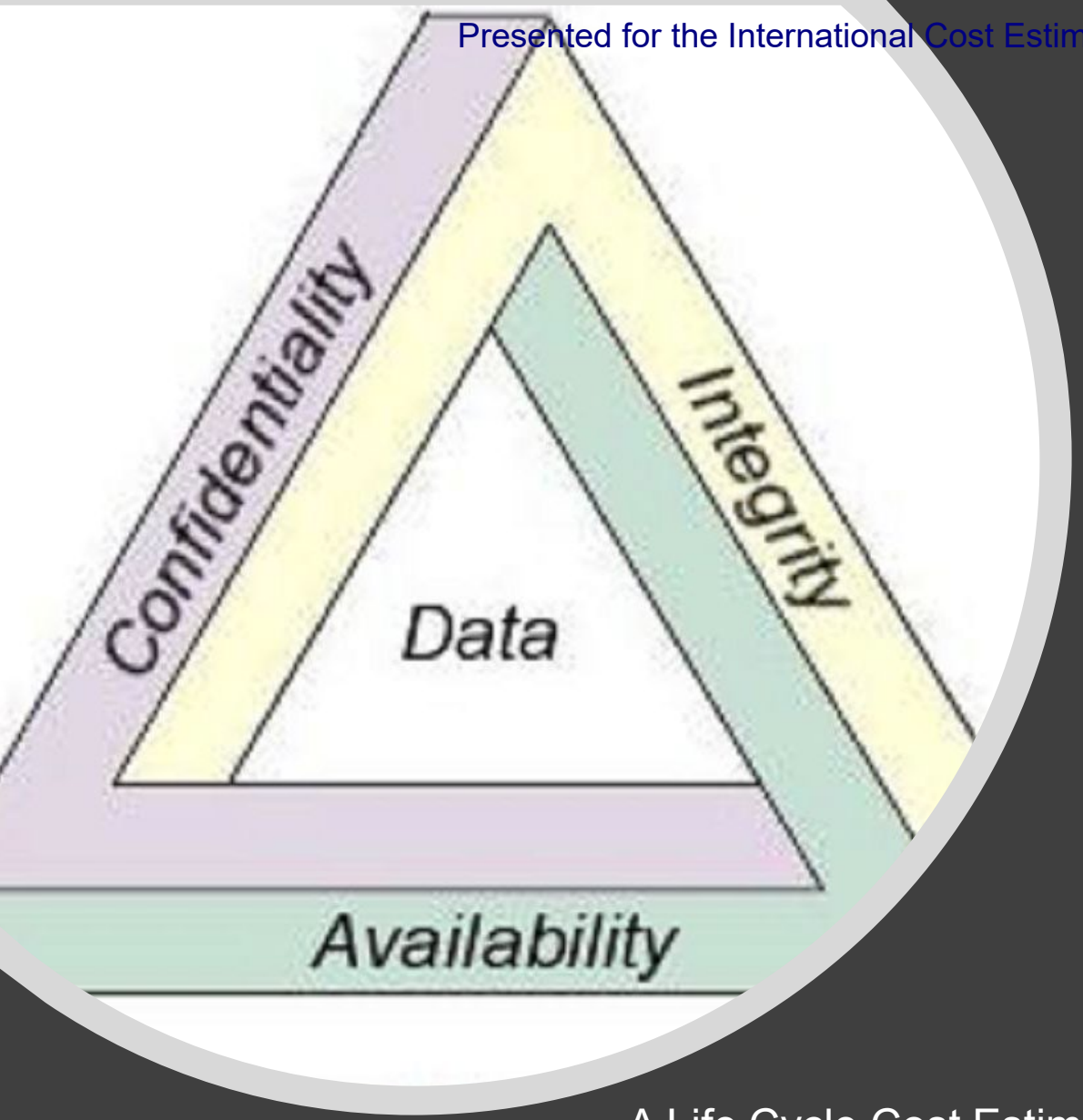


Recommended Reading
The Biggest Myth Continued

"I would say that the biggest myth about cybersecurity is that spending more money makes you more secure. Many companies are willing to spend their money on expensive products when they should focus their efforts on hiring educated and talented employees."

"The most recurring myth I encounter is that security isn't everyone's problem. The reality is that using secure and privacy-enabling technology isn't just beneficial for yourself, but it is, in practice, an act of solidarity."

Bottom Line: Cybersecurity is not hard it is a marathon

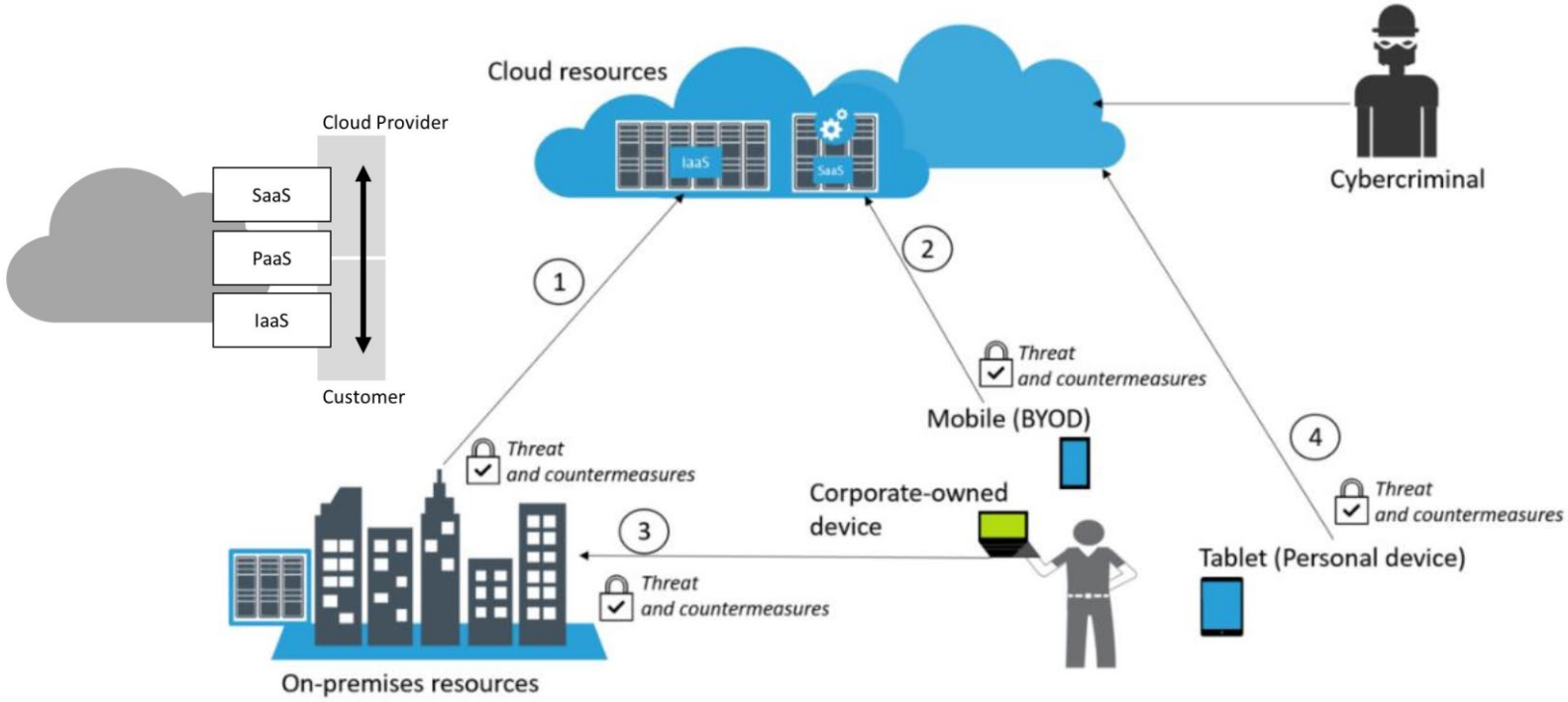


Cybersecurity

- Cyber Security means different things to different sets of people, e.g.
  - personal,
  - small business,
  - large business,
  - national security, …
- Information security performs four important functions for an organization:
  - Protecting the organization's ability to function
  - Protecting the data and information the organization collects and uses
  - Enabling the safe operation of applications running on the organization's IT systems
  - Safeguarding the organization's technology assets
- Includes
  - Physical security/Infrastructure
  - Local Hosts
  - Local Networks
  - Perimeter

A Life Cycle Cost Estimate should address all costs; Protection, Detection, and Response

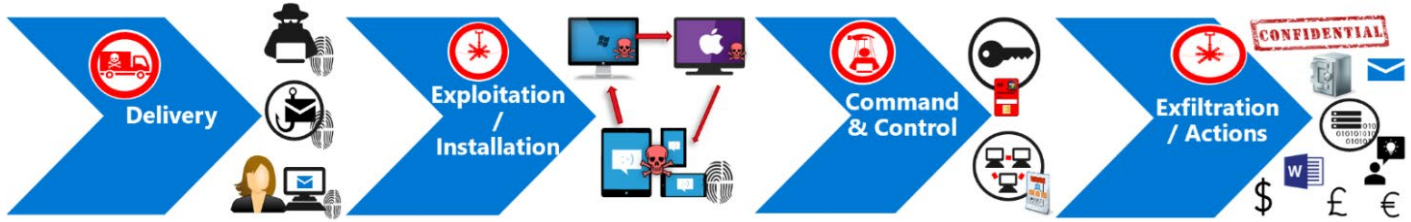
Correlation Between Attacks and User*



- Information systems now are so complicated that U.S. companies need more than 200 days, on average, just to detect a breach.
- On average 75% of attacks are External and 25% Internal.
- With more “remote” work, there will be more vulnerability

*Diogenes, Yuri. Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition . Packt Publishing. Kindle Edition.

CYBER Kill Chain & Threat Actors



Your security posture won't be fully completed if you don't have a good detection system; this means having the right sensors distributed across the network, monitoring the activities.

Diogenes, Yuri. Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition

Central Cyber Threats

Every cyber decision hinges upon two questions:

Will it work, and is it affordable

Key Threat Actors

Some threats are easier to cost than others

It is not just about hardware/software solutions

Some suggest the cost of protection is greater than the cost to develop a threat

Real World Case of Ransomware

WannaCry

At this point, the incident response team was working on three different fronts: one to try to break the ransomware encryption, another to try to identify other systems that were vulnerable to this type of attack, and another one working to communicate the issue to the press.

Diogenes, Yuri. Cybersecurity – Attack and Defense Strategies: Counter modern threats and employ state-of-the-art tools and techniques to protect your organization against cybercriminals, 2nd Edition . Packt Publishing. Kindle Edition.

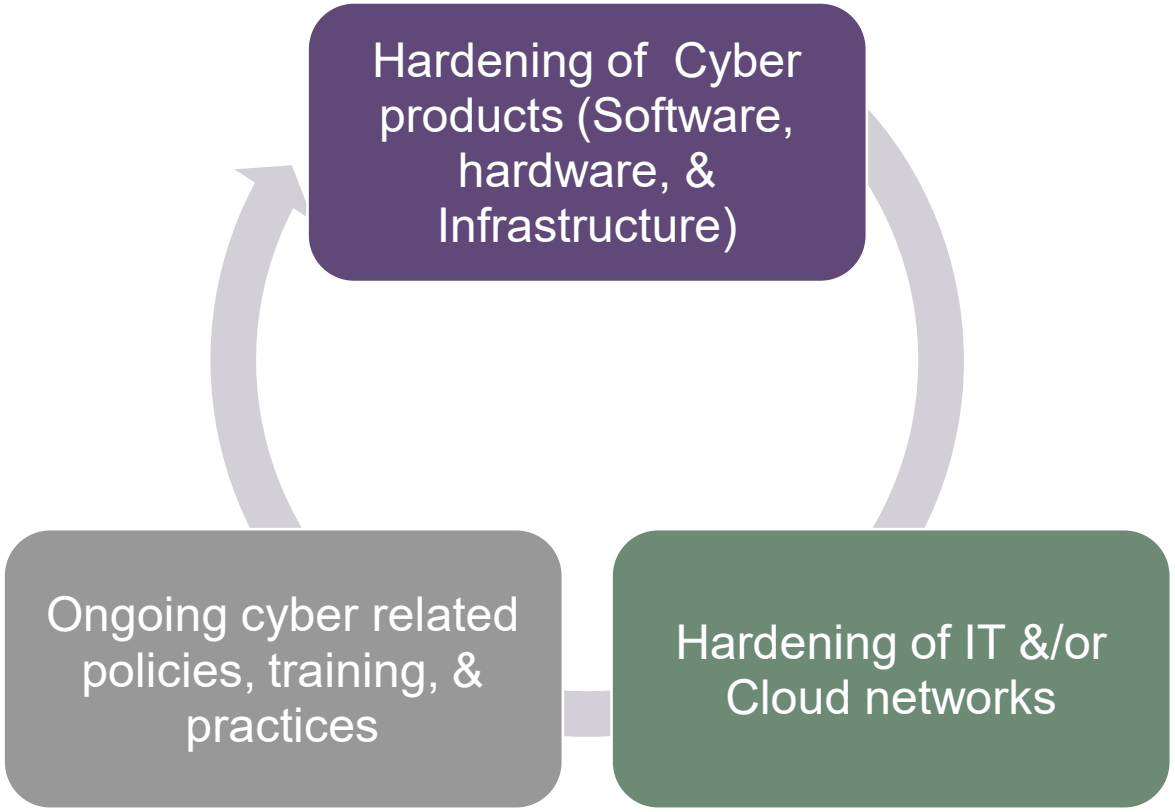
GALORATH

Approaches To Cybersecurity Cost Analysis

- Economic/Cost Benefit Model – excellent for some business decisions – however, some benefits (life, safety, security) are difficult to quantify
- Bottoms-Up/Engineering Build Up Model – great way to effectively cost what is defined – however, we face the classic “know, unknown, and unknown-unknown issue”*
- Top-Down/Parametric Model – based on statistically valid cause and effect relationships – however, data is the key

*In a news briefing in February 2002, the United States Secretary of Defense, Donald Rumsfeld, responded to a question with a phrase that continues to be used even today by the intelligence community. He said: "As we know, there are known knowns; there are things we know we know. We also know there are known unknowns; that is to say we know there are some things we do not know. But there are also unknown unknowns—the ones we don't know we don't know."

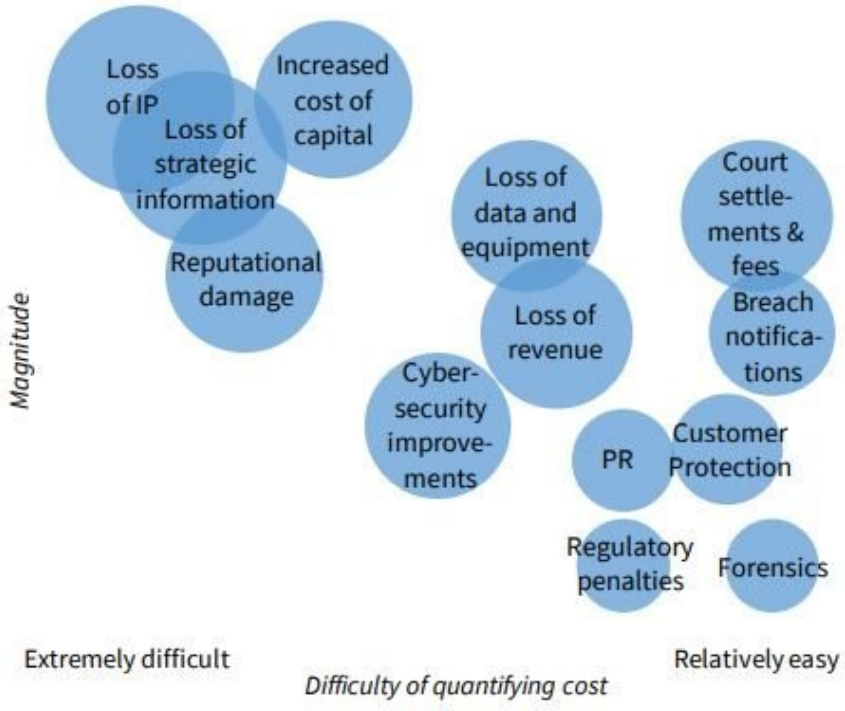
Cybersecurity Costing Includes Infrastructure, People, Software, Hardware, IT & Policy, and Threat Life Cycle Management



Cost Impacts of An Adverse Cyber Event*

- Forensics

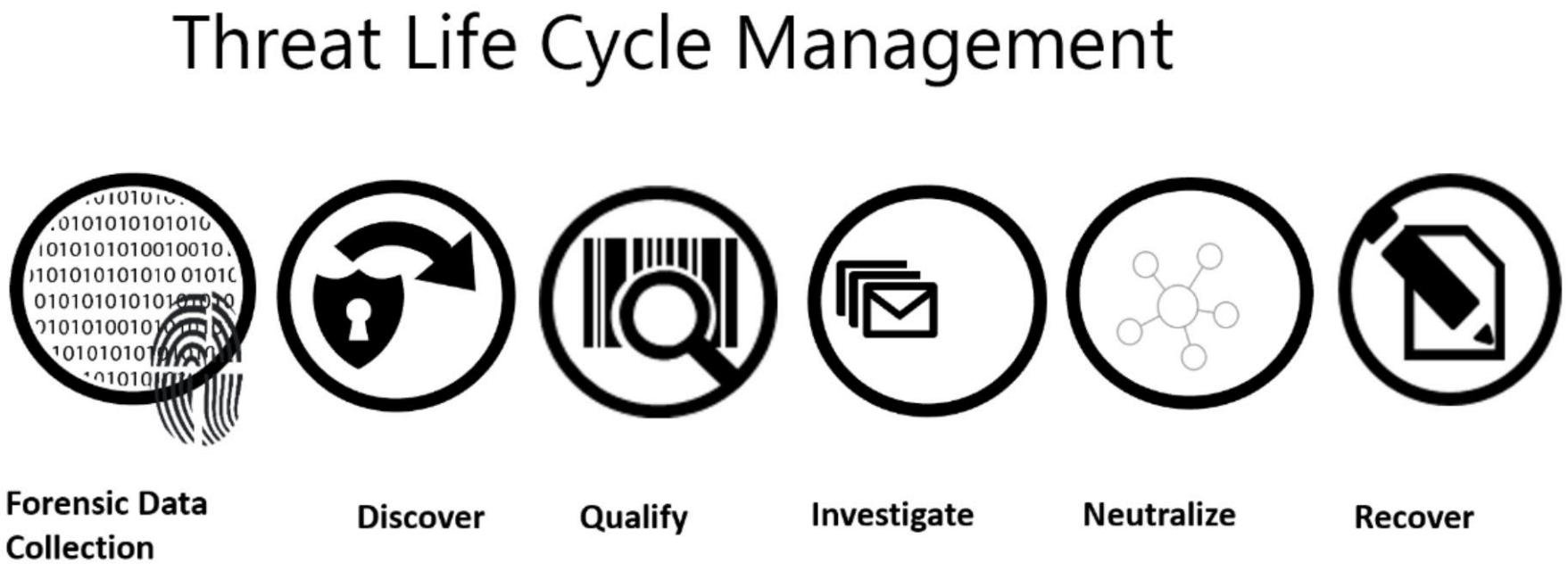
(The Cost of Malicious Cyber Activity to the U.S. Economy - Feb 2018)



Above costs don't include cost impact of breaches

The O&S/TOC/Sustainment of Cybersecurity

Sometimes we think of Cybersecurity as the defensive posture only, rather than considering the total life cycle



MITRE ATTCK FRAMEWORK

Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Exfiltration	Command And Control
10 items	31 items	56 items	28 items	59 items	20 items	19 items	17 items	13 items	9 items	21 items
Drive-by Compromise	AppleScript	.bash_profile and .bashrc	Access Token Manipulation	Access Token Manipulation	Account Manipulation	Account Discovery	AppleScript	Audio Capture	Automated Exfiltration	Commonly Used Port
Exploit Public-Facing Application	CMSTP	Accessibility Features	Accessibility Features	Binary Padding	Bash History	Application Window Discovery	Application Deployment Software	Automated Collection	Data Compressed	Communication Through Removable Media
Hardware Additions	Command-Line Interface	AppCert DLLs	AppCert DLLs	BITS Jobs	Brute Force	Browser Bookmark Discovery	Distributed Component Object Model	Clipboard Data	Data Encrypted	Connection Proxy
Replication Through Removable Media	Control Panel Items	AppInit DLLs	AppInit DLLs	Bypass User Account Control	Credential Dumping	File and Directory	Exploitation of Remote Services	Data from Information Repositories	Data Transfer Size Limits	Custom Command and Control Protocol
Spearphishing Attachment	Dynamic Data Exchange	Application Shimming	Application Shimming	Clear Command History	Credentials in Files		Logon Scripts	Data from Local System	Exfiltration Over Alternative Protocol	Custom Cryptographic Protocol
Spearphishing Link	Execution through API	Authentication Package	Bypass User Account Control	CM			Pass the Hash	Data from Network Shared Drive	Exfiltration Over Command and Control Channel	Data Encoding
Spearphishing via Service	Execution through Module Load	BITS Jobs	DLL Search Order Hijacking	Co			Pass the Ticket	Data from Removable Media	Exfiltration Over Other Network Medium	Data Obfuscation
Supply Chain Compromise	Exploitation for Client Execution	Bootkit	Dylib Hijacking	Co			Remote Desktop Protocol	Data Staged	Exfiltration Over Physical Medium	Domain Fronting
Trusted Relationship	Graphical User Interface	Browser Extensions	Exploitation for Privilege Escalation	Co			Remote File Copy	Email Collection	Scheduled Transfer	Fallback Channels
Valid Accounts	InstallUtil	Change Default File Association	Extra Window Memory Injection	Co			Remote Services	Input Capture		Multi-hop Proxy
	Launchctl	Component Firmware	File System Permissions Weakness	Hi			Replication Through Removable Media	Man in the Browser		Multi-Stage Channels
	Local Job Scheduling	Component Object Model Hijacking	Hooking				Shared Webroot	Screen Capture		Multiband Communication
	LSASS Driver	Create Account	Image File Execution Options Injection	Dl			SSH Hijacking	Video Capture		Multilayer Encryption
	Mshta	DLL Search Order Hijacking	Launch Daemon				Taint Shared Content			Port Knocking
	PowerShell	Dylib Hijacking	New Service	Ex			Third-party Software			Remote Access Tools
	Regsvcs/Regasm	External Remote Services	Path Interception	Ext			Windows Admin Shares			Remote File Copy
	Regsvr32	File System Permissions Weakness	Plist Modification	Fil			Windows Remote Management			Standard Application Layer Protocol
	Rundll32	Hidden Files and Directories	Port Monitors	File System Logical Offsets						Standard Cryptographic Protocol
	Scheduled Task	Hooking	Process Injection	Gatekeeper Bypass						Standard Non-Application Layer Protocol
	Scripting	Hypervisor	Scheduled Task	Hidden Files and Directories						Uncommonly Used Port
	Service Execution	Image File Execution Options Injection	Service Registry Permissions Weakness	Hidden Users						Web Service
	Signed Binary Proxy Execution	Kernel Modules and Extensions	Setuid and Setgid	Hidden Window						
	Signed Script Proxy Execution	Launch Agent		HISTCONTROL						
	Source			Image File Execution Options Injection						
	Space after Filename									

MITRE

ATT&CK™

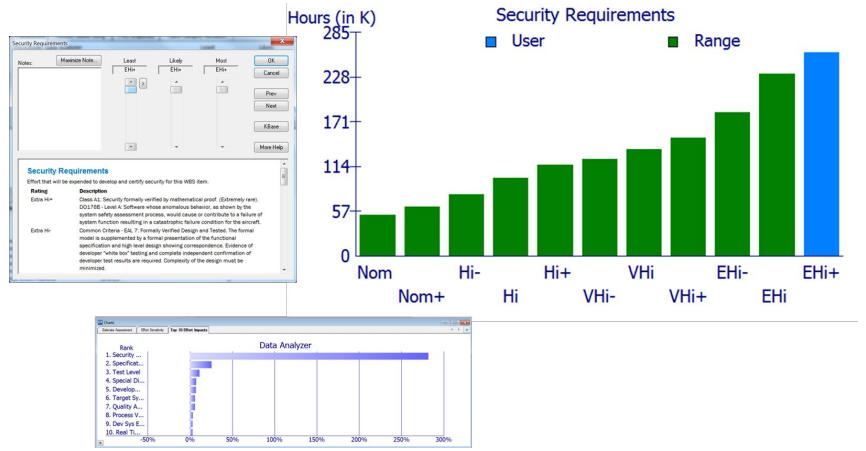
Adversarial Tactics, Techniques & Common Knowledge

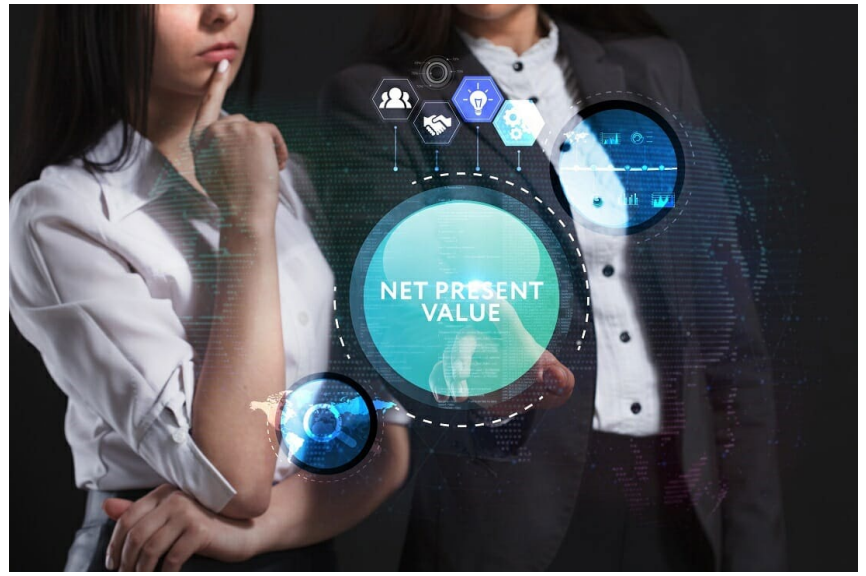
GALORATH

Today Cybersecurity Costs are being assessed in two primary ways:

- Traditional WBS Build Up – “Bottom Up” engineering build up – Galorath is building a database/repository of Cybersecurity items and implementing solutions in SEER
- Cost Risk/NPV – Economic Value Assessment – cost per breach

We are missing a “Top Down/Parametric” approach to Cybersecurity Cost Analysis





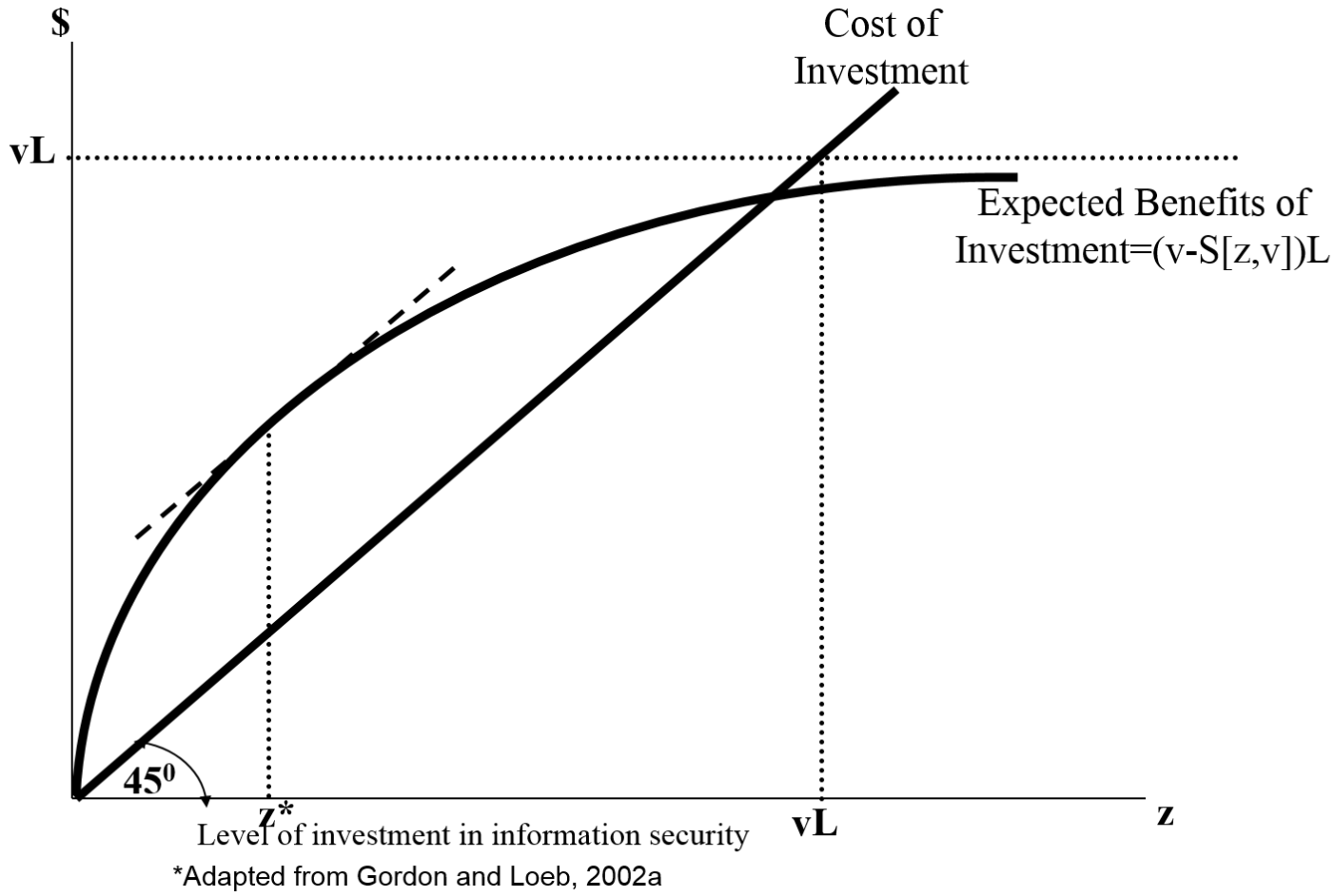
Economic/Cost Benefit Model

Key Economic Measures

- **Net Present Value**
- **Internal Rate of Return**
- **Return On Investment**

One key finding from the Gordon and Lobe model is: ***"The amount a firm should spend to protect information is generally no more that one-third or so (37%)of projected loss from a breach. Above that level, in most cases, each dollar spent will reduce the anticipated loss by less than a dollar."***

There are some hard decisions, e.g. What is yo*ur* reputation worth?



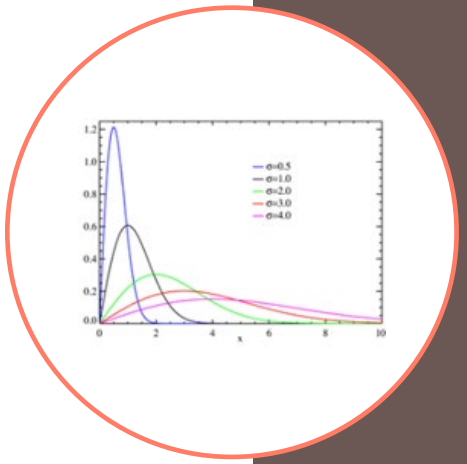
*Adapted from Gordon and Loeb, 2002a

Conceptual "Parametric" Cyber Cost Analysis Model

- Generic COCOMO Approach - **E=*ai*(KLoC)*(bi)*(EAF)**
  - where E is the effort applied in person-months, **KLoC** is the estimated number of thousands of delivered lines of code for the project, and **EAF** is the factor calculated above.

- Simply described*
  - Size (Measured as LOC, FP, SP, …) is run through a set of environmental factor to produce an effort and the effort is distributed over time using a statistical distribution
  - Could we apply this conceptual approach to developing a Cyber Model?**

- A CO"CYBER"MO



* With deep apologies to all COCOMO/Software cost experts

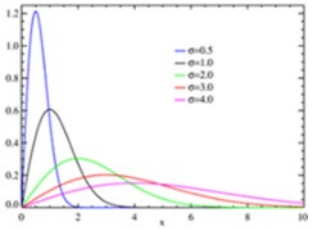
** With recognition that USC is already proposing a common criteria evaluation assurance levels (CC EAL) model

Cybersecurity Variables

- Sectors – National Security, Commercial, Other Federal (these sectors will expand as we collect data)
- Threat Actors - Nation States, Competitors, Criminals, Hacktivists, Opportunists, and Insiders (will this set of threats change/grow)
- Cyber Mitigations/Evaluations – Physical Security, Network Security, Education, Malware, Removable media, Secure config, User privileges, Monitoring, and Remote Working

The Hypothetical "SECURE" Cyber Cost Model (Sector Evaluated Cyber Utility Risk Estimate)

A	B	C	D	E	F	G	Model
					Cost for each evaluation **		
SECTOR*	THREAT ACTORS	Risk Assessment	10 Step Evaluation For each threat	Low	Med	High	Output
1. National Security	Nation States	R1 (%)	Physical Security				
	Competitors	R2 (%)	Network Security	$	$	$	
	Criminals	R3 (%)	Education	$	$	$	Low Med High
	Hacktivists	R14(%)	Malware	$	$	$	Sum of the products of each row
	Opportunists	R15(%)	Removable media	$	$	$	
	Insiders	R6 (%)	Secure config	$	$	$	
			User privileges	$	$	$	
		SUM = 100%	Monitoring				
			Remote Working				
2. Commercial							
3. Federal (Other)							

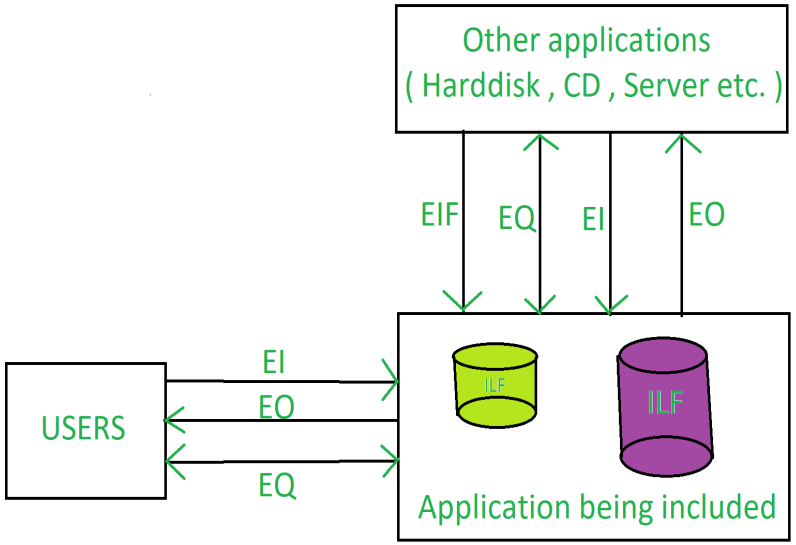


* Multiple Sectors could be evaluated at the same time; e.g. a commercial company developing a National Security product
* *need Data Collection

GALORATH

An Alternative Cost Model

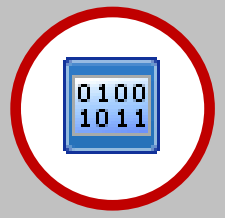
- During an ISBGS presentation they proposed a function point approach



In either case we need to identify cost drivers and then collect and analyze data

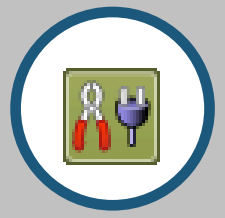
THE SEER SUITE

Predictive Analytics for Various Domains



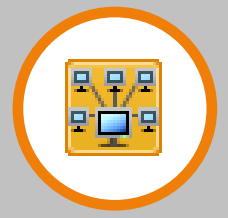
SEER-SEM

Software/application development, maintenance, integration and testing for Total Ownership Cost



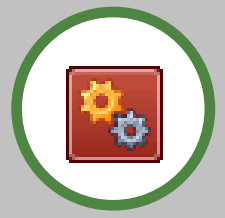
SEER-H

System, hardware and electronics development, production and support for Total Ownership Cost



SEER-IT

IT infrastructure, services and operations including Service desk, Tier 1-3 support, and ongoing support



SEER-MFG

Hardware manufacturing and assembly with automated CAD to Cost

SEER-SYS

Systems Engineering cost estimation for systems of all sizes and complexities

SEER-SPACE

Estimates entire lifecycle cost for key instruments and spacecraft subsystems

Soon to add SEER SECURE

GALORATH