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
Agenda

• Background and Example – slides 2 - 8
• Attacks and Threats – slides 9 -12
• Cost Approaches and Shortfalls – slides 13 – 17
• New Hypothetical Model – slides 18 - 23
Cybersecurity is critical to all areas

Key National Security Initiatives
- Space Dominance
- Data Analytics/Data Science
- Cybersecurity

Space Dominance  
Data Analytics/Data Science

Cybersecurity is critical to all areas
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)
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.

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
Every cyber decision hinges upon two questions:
Will it work, and is it affordable

Key Threat Actors

Central Cyber Threats

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
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.

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

Above costs don’t include cost impact of breaches

Cost Impacts of An Adverse Cyber Event*
- Forensics

(The Cost of Malicious Cyber Activity to the U.S. Economy - Feb 2018)
The O&S/TOC/Sustainment of Cybersecurity

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

Threat Life Cycle Management

- Forensic Data Collection
- Discover
- Qualify
- Investigate
- Neutralize
- Recover
MITRE ATTCK FRAMEWORK

<table>
<thead>
<tr>
<th>Initial Access</th>
<th>Execution</th>
<th>Persistence</th>
<th>Privilege Escalation</th>
<th>Defense Evasion</th>
<th>Credential Access</th>
<th>Discovery</th>
<th>Lateral Movement</th>
<th>Collection</th>
<th>Exfiltration</th>
<th>Command And Control</th>
</tr>
</thead>
<tbody>
<tr>
<td>10 Items</td>
<td>31 Items</td>
<td>56 Items</td>
<td>23 Items</td>
<td>28 Items</td>
<td>59 Items</td>
<td>20 Items</td>
<td>18 Items</td>
<td>17 Items</td>
<td>11 Items</td>
<td>9 Items</td>
</tr>
<tr>
<td>Drive-by Compromise</td>
<td>CMIP</td>
<td>Credibility</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Exploit Public-Facing Application</td>
<td>Command-Line Interface</td>
<td>Dynamic Data Exchange</td>
<td>Execution through API</td>
<td>Bypass User Account Control</td>
<td>Account Discovery</td>
<td>Application Window Discovery</td>
<td>Audio Capture</td>
<td>Automated Collection</td>
<td>Commonly Used Port</td>
<td></td>
</tr>
<tr>
<td>Hardware Additions</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Replication Through Removable Media</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing Attachment</td>
<td>Spearphishing Link</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Spearphishing via Service</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Supply Chain Compromise</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Trusted Relationship</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Valid Accounts</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

MITRE ATT&CK™
Adversarial Tactics, Techniques & Common Knowledge

![MITRE ATT&CK Diagram](image-url)
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 than 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 your reputation worth?

*Adapted from Gordon and Loeb, 2002a
Conceptual “Parametric” Cyber Cost Analysis Model

• Generic COCOMO Approach - $E = a_i(KLoC)(b_i)(EAF)$
  • 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)

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

<table>
<thead>
<tr>
<th>SECTOR*</th>
<th>THREAT ACTORS</th>
<th>Risk Assessment</th>
<th>10 Step Evaluation For each threat</th>
<th>E</th>
<th>F Cost for each evaluation **</th>
<th>G</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. National Security</td>
<td>Nation States</td>
<td>R1 (%)</td>
<td>Physical Security</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td>Low</td>
</tr>
<tr>
<td></td>
<td>Competitors</td>
<td>R2 (%)</td>
<td>Network Security</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Criminals</td>
<td>R3 (%)</td>
<td>Education</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Hacktivists</td>
<td>R14(%)</td>
<td>Malware</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Opportunists</td>
<td>R15(%)</td>
<td>Removable media</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Insiders</td>
<td>R6 (%)</td>
<td>Secure config</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>User privileges</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Monitoring</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Remote Working</td>
<td>$</td>
<td>$</td>
<td>$</td>
<td></td>
</tr>
<tr>
<td>SUM = 100%</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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
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