Technomics
Better Decisions Faster

Advancing the Art of Cybersecurity Cost Estimating

New Considerations for Structure and Assumptions

ICEAA Workshop
Minneapolis, MN

May 15th, 2024

Agenda

- Introduction: Why is Cyber Cost Important?
- Emerging Cyber Initiatives
- Introduction to Secure Software WBS
- Case Study Application
- Limitations
- Conclusion

Team

Austin MacDougall

Mr. MacDougall is a CCEA and SCEC certified cost analyst with over 6 years of professional experience spanning IT cost estimating and analysis, agile software implementation support, and program management support. During his time at Technomics, Austin has supported a number of clients in the federal space, including DHS, FEMA, CBP, and others. He has a Bachelor's Degree from Dickinson College.

William Gellatly

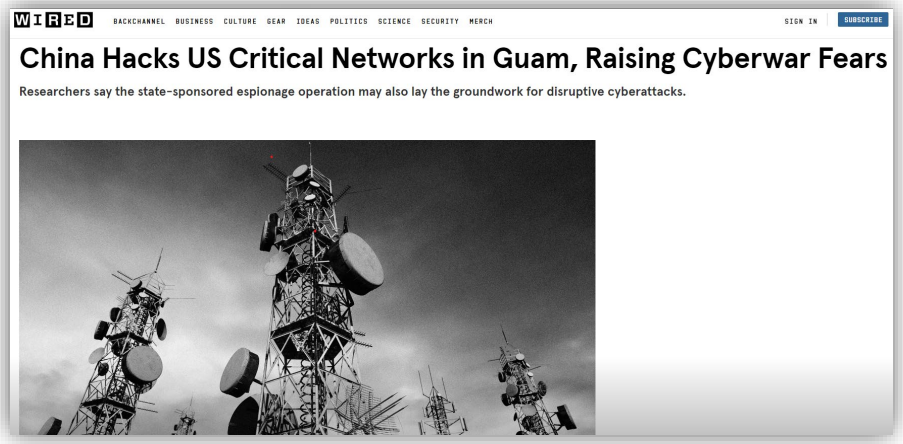
William Gellatly is a SCEC certified analyst with more than 10 years of experience in IT estimation support and analysis for multiple government agencies including DHS, USPS and the U.S. Census Bureau. William holds a Bachelor's Degree in History and Political Science from Guilford College and a Master of Science in Information Technology and Management from the University of North Carolina at Greensboro.

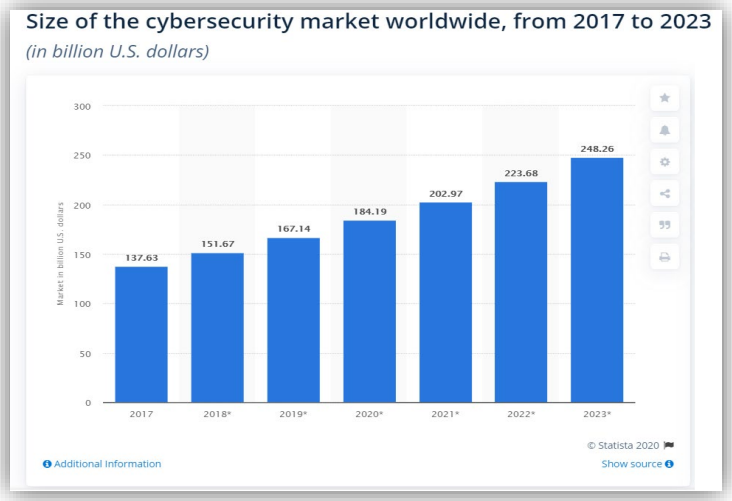
Jessica Kleinman

Jessica Kleinman has over 4 years of experience providing decision support for several defense agencies as well as DHS CISA. She has experience in cost estimating, budget analysis, data warehouse development and maintenance, and program management support. She holds a Bachelor's Degree in Economics from Georgia College & State University.

Why is Cyber Cost Important?

- Recent high-profile incidents have led to significant remediation costs and produced reputational damage – and the number of incidents is growing
- These incidents drove federal and private-sector organizations to invest in protection against future attacks
- At the same time, costs of cybersecurity – particularly in the development phase – are not well defined



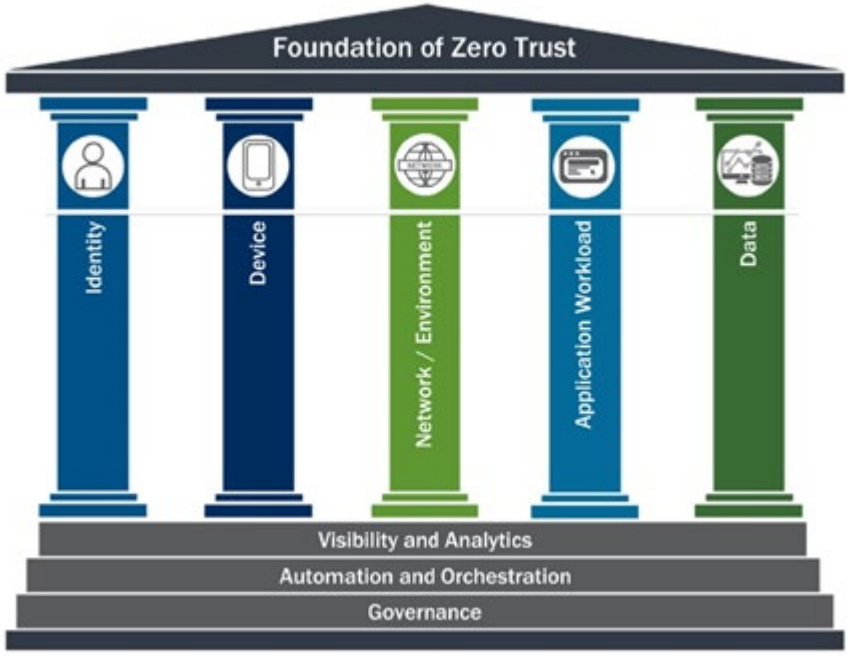


Emerging Cyber Initiatives

- New cyber best practices emphasize earlier, more proactive approaches to cybersecurity:
  - Increased authentication (Zero Trust Architecture - ZTA)
  - Emphasis on secure development and configuration (Secure by Design)
- Understanding these trends is important to evaluating the scope of a program's security requirement

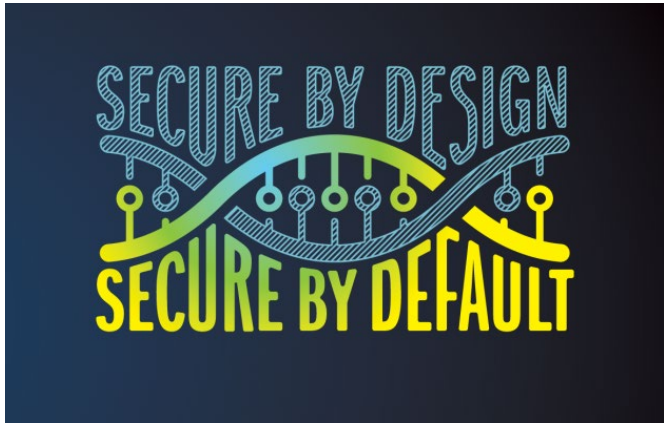
Zero Trust Architecture

- **Zero Trust**: an authentication paradigm that requires continued re-authentication of all assets on a network
- Evolution from prior perimeter-based “implicit trust” model to a “trust, but verify” approach:
  - **Perimeter**: a logical boundary within which a particular security policy is applied
  - **Trust, but Verify**: all items, including those within a network, have the potential to be compromised



Secure by Design

- A posture that emphasizes correcting cybersecurity vulnerabilities as a built-in requirement for new software development
- Paradigm- and platform-agnostic
- Common tasks include application hardening and secure default settings
- Limits on programming languages to prevent memory safety vulnerabilities



Challenges in Cost Estimating

- New initiatives = minimal historical cost data
- Lack of common estimating structures
- For cybersecurity cost methodology to improve, requirements must be better defined, and more cost data must be collected

SSDF Intro

- Secure Software Development Framework (SSDF), produced by National Institute for Standards and Technology (NIST)
- Identifies secure software development practices throughout the Software Development Life Cycle (SDLC)
- Considered an authoritative source for development phase cybersecurity practice, particularly for Secure by Design

SSDF Category	SSDF Definition	Generalized WBS Crosswalk
Prepare the Organization (PO)	Prepare people, processes, and technology to perform secure software development at organization level.	Systems Engineering, System Development, System Procurement, Training
Protect the Software (PS)	Protect all components of software from tampering and unauthorized access.	System Development, Data Center Support
Produce Well-Secured Software (PW)	Produce well-secured software with minimal security vulnerabilities in releases.	System Development, System Procurement, Testing
Respond to Vulnerabilities (RV)	Identify residual vulnerabilities in software releases and respond appropriately to address and prevent recurrence.	Sustainment-Phase Systems Engineering, SOC Support

Secure Software WBS

- Adapted from NIST SSDF, to accommodate standard product-oriented software development and sustainment Work Breakdown Structure (WBS)
- Sample IT WBS in crosswalk represents WBS developed by Department of Homeland Security (DHS) Cost Analysis Division (CAD)

Development:

Secure Software WBS:

ID	Name
1.0	**Development-Phase Security Activities**
1.1	**Cybersecurity Engineering**
1.2	**Secure Software Design**
1.3	**Secure Software Development**
1.4	**Secure Software Procurement**
1.5	**Secure Hosting Support**
1.6	**Security Testing**
1.7	**Security Training**

Sample IT WBS (DHS)

ID	Name
1.0	**Investment**
1.i…n+1	[System Sub-Sections, if needed]
1.i.1	Program/Project Management
1.i.2	Systems Engineering (or Systems Analysis)
1.i.3	Business Process Re-Engineering/Change Management
1.i.4	System Development
1.i.5	System Procurement
1.i.6	Central Data Center Investment
1.i.7	System Level Integration & Test
1.i.8	System Deployment/Implementation
1.i.9	System Documentation & Related Data
1.i.10	Other Investment

Sustainment

Secure Software WBS:

ID	Name
2.0	**Sustainment-Phase Security Activities**
2.1	**Cybersecurity Engineering (OM)**
2.2	**Security Operations Center Support**
2.3	**Security Software Sustainment**

Sample IT WBS (DHS)

ID	Name
2.0	**Investment**
2.i…n+1	[System Sub-Sections, if needed]
2.i.1	Program/Project Management
2.i.2	Systems Engineering (or Systems Analysis)
2.i.3	Business Process Re-engineering / Change Management
2.i.4	Help Desk/Service Desk Support
2.i.5	Annual Operations Procurement & Leasing
2.i.6	Central Data Center Operating Support
2.i.7	Technology Refresh/Upgrade
2.i.8	System Maintenance
2.i.9	System Documentation & Related Data
2.i.10	System Data Maintenance
2.i.11	Site Operations
2.i.12	Other Operations & Maintenance

Secure Software WBS

ID	Name	Source Crosswalk
1.0	**Development-Phase Security Activities**	Roll-Up
1.1	**Cybersecurity Engineering**	Roll-Up
1.1.1	Security Requirements Definition	SSDF PO.1.1, PO.1.2, PO.1.3
1.1.2	Determine Roles and Responsibilities	SSDF PO.2.1, PO.2.3
1.1.3	Determine Supporting Toolchains	SSDF PO.3.1
1.1.4	Define Security Check Criteria	SSDF PO.4.1
1.2	**Secure Software Design**	Roll-Up
1.2.1	Risk Analysis and Mitigation	SSDF PW.1.1, PW1.2, PW.1.3
1.2.2	Independent Verification and Validation	SSDF PW.2.1
1.3	**Secure Software Development**	Roll-Up
1.3.1	Software Security Check Development	SSDF PO.4.2.
1.3.2	Implement and Configure Toolchains	SSDF PO.3.2, PO.3.3
1.3.3	Secure Source Code	SSDF PW.5.1, PW.7.1, PW.7.2
1.3.4	Software Code Protection	SSDF PS.1.1, PS.1.2
1.3.5	Develop Secure Software	SSDF PW.4.2
1.3.6	Configure Compile-Interpret-Build Tools	SSDF PW.6.1, PW.6.2
1.4	**Secure Software Procurement**	Roll-Up
1.4.1	Commercial Security Software Purchases	SSDF PW.4.1, PW.4.4
1.4.2	Secure-by-Default Configuration	SSDF PW.9.1, PW.9.2
1.4.3	Security Hardware Appliances	SSDF PW.4.1, PW.4.4

ID	Name	Source Crosswalk
1.5	**Secure Hosting Support**	Roll-Up
1.5.1	Secure Environment and Endpoints	SSDF PO.5.1, PO.5.2
1.5.2	Release Archiving	SSDF PS.3.1, PS.3.2
1.6	**Security Testing**	Roll-Up
1.6.1	System Security Testing	SSDF PW.8.1. PW.8.2
1.7	**Security Training**	Roll-Up
1.7.1	Security Training	SSDF PO.2.2
2.0	**Sustainment-Phase Security Activities**	Roll-Up
2.1	**Cybersecurity Engineering (OM)**	Roll-Up
2.1.1	Ongoing Security Assessments	SSDF RV.1.1., RV.1.2
2.2	**Security Operations Center Support**	Roll-Up
2.2.1	Monitoring Support (Threat Hunting and Assessment)	SSDF RV1-3
2.2.2	Incident Support (Incident Response/Recovery)	SSDF RV1-3
2.2.3	Threat Information Data Acquisition/Subscription	SSDF RV1-3
2.3	**Security Software Maintenance**	Roll-Up
2.3.1	Security Software Sustainment	SSDF PW.4.1, PW.4.4
2.3.2	Security Hardware Sustainment	SSDF PW.4.1, PW.4.4

Practical Application Intros

- Sufficient data does not yet exist for detailed methodology and Cost Estimating Relationship (CER) development
- Hypothetical case studies are displayed to illustrate how WBS is applied to cybersecurity cost categories
- WBS is summarized at Level 2, assume similar methodology applies at lower levels except where otherwise noted

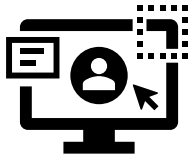
Case Study Application

Case Study 1

- Shipment tracking system for a logistics agency
- New software development to Secure by Design standards
- Cloud hosting environment, with stand-alone Security Operations Center (SOC)
- Requirements documentation, such as an Operational Requirements Document (ORD) or Concept of Operations (CONOPS) available for functional size
- A similar (albeit smaller) program was completed by the organization with cost data available

Case Study 2

- Federal organization IT asset management system in sustainment
- Currently upgrading from perimeter-based architecture to Zero Trust architecture
- Along with Zero Trust development, assess routine processes for security vulnerabilities
- System size in Equivalent Source Lines of Code (ESLOC) and operating costs are known, along with ZTA development costs for other systems in organization



WBS 1.1 – Cybersecurity Engineering

- Early-stage efforts associated with assessing the security requirements for a secure software development effort
- Primary driver is labor, best measured by security team size and frequency of Authority to Operate (ATO) renewal

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Pre-design assessments to understand scope of requirements needed to incorporate ZTA and Secure by Design approaches into development. Criteria may be indicated in a program Requirements document.	**Primary:** use scaled analogy data from prior program to estimate cyber engineering team size. **Secondary:** quantify security requirements from CONOPS/FRD, including frequency of ATO/security renewals.
Case Study 2 	Primary effort involves engineering for ZTA optimization. Secondary efforts include proactive assessment of system for additional vulnerabilities. Any additional vulnerabilities are flagged for subsequent Design/Development sections.	**Primary**: adjust staff costs current security team to include expanded scope or ZTA development. **Secondary**: quantify security requirements from CONOPS/ORD, including frequency of ATO/security renewals.

WBS 1.2 – Secure Software Design

- Efforts to design software that is well-secured and proactively addresses potential vulnerabilities
- Includes cyber risk analysis and Independent Verification and Validation (IV&V) activities

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Design of how security requirements identified in Cybersecurity Engineering category can be integrated into broader design and architecture of the system.	**Primary**: use results from Cyber Engineering assessment activities, including number of identified vulnerabilities. **Secondary**: use system size as measured by Function Points (FP) and number of interfaces for scaled analogy.
Case Study 2 	Redesign of existing system components, determination of ZTA boundaries.	**Primary**: use results from Cyber Engineering assessment activities, including number of identified vulnerabilities. **Secondary**: se system size as measured by Function Points (FP) and number of interfaces for scaled analogy.

WBS 1.3 – Secure Software Development

- Includes software development effort that involves modifying the code of the system.
- Does not include Commercial Off-The-Shelf (COTS) software license costs (in WBS 1.4)

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Develop security functionality as part of broader application development process.	**Primary**: output from Cyber Engineering assessment activities used for Secure Software Design, with any additional effort added from Risk Assessment/IV&V. **Secondary**: use system size as measured by Function Points (FP) and number of interfaces for scaled analogy.
Case Study 2 	Primary effort includes development and integration of new functionality for ZTA. Secondary effort includes execution of any vulnerability remediation flagged in Cybersecurity Engineering category.	**Primary**: use results from Cyber Engineering assessment activities used for Secure Software Design, with any additional effort added from Risk Assessment/IV&V. **Secondary:** use system size as measured by Function Points (FP) and number of interfaces for scaled analogy.

WBS 1.4 – Secure Software Procurement

- Includes purchase, configuration, and integration of Commercial Off-The-Shelf (COTS) security software

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Purchase of new COTS licenses for cybersecurity functions (Authentication, Encryption, Monitoring, Intrusion Protection). New development effort assumes 0 pre-existing licenses available.	**Primary**: determine license criteria for Cost-per-License estimate. Potential drivers include number of users, number of servers, number of endpoints/connections, dependent on vendor pricing structure. **Secondary**: number of system users
Case Study 2 	Purchase of new COTS license types and increased quantity of existing licenses. For ZTA, heavy focus on authentication software such as Single Sign On (SSO) and Multi-Factor Authentication (MFA).	**Primary**: determine license criteria for Cost-per-License estimate for any new licenses. Potential drives include number of users, number of servers, number of endpoints/connections, dependent on vendor pricing structure. **Secondary**: use number of users for scaled analogy for prior programs that completed ZTA re-architecture.

WBS 1.5 – Secure Hosting Support

- Represents security-related efforts needed to secure a hosting environment, harden endpoints, and perform related security tasks
- Most potential costs apply to both on-premise and cloud hosting platforms

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Additional labor during hosting stand-up to ensure that hosting environment and endpoints are set up and configured securely.	**Primary**: determine based on hosting size data, such as number of servers, processing cores, and/or virtual machines. **Secondary**: number of system users
Case Study 2 	Minor re-configuration of environment, assumes limited “new” effort needed.	Minimal direct cost assumed, but hosting footprint may need to expand to host new security software beyond expected hosting growth.

WBS 1.6 – Security Testing

- Represents integration and testing activities conducted to validate a system's compliance with security requirements
- Includes design and performance of security tests, including those needed to obtain initial Authority to Operation (ATO)

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	All applicable security test events conducted, with issues adjudicated by development team.	**Primary**: using Test Plan or similar documentation, assume number of cybersecurity test cases drives security testing cost. **Secondary**: leverage analogous cyber testing data or use system sizing estimate and analogous system testing factor.
Case Study 2 	Testing of any changes made in Development process to ensure no inadvertent damage to functionality or system security.	**Primary**: number of test cases if Testing Plan is available. **Secondary**: extrapolate from past actuals, adjust to accommodate adds, removals, and changes to security testing made during ZTA development.

WBS 1.7 – Security Training

- Represents effort required to develop and conduct role-based security training

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Develop and conduct training for any new user roles created by the new system.	**Primary**: number of training products needed for security-related training curriculum. Determine if using in-person Instructor Led Training (ILT), webinar, or video training. **Secondary**: number of system users
Case Study 2 	Likely no need training events, other than process knowledge for end-user Help Desk (not in scope) and Security Operations Center (SOC) (possibly in scope).	Minimal direct cost assumed but determine if training module updates exceed normal training update effort.

WBS 2.1 – Cybersecurity Engineering (OM)

- Represents sustainment phase security systems engineering effort, including Authority to Operate (ATO) renewal

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Sustainment-phase security engineering activities, including operational security assessments and renewal of system ATO.	**Primary**: measure frequency of ATO/security renewals. **Secondary:** use scaled analogy data from prior program to estimate cyber engineering team size.
Case Study 2 	Sustainment-phase security engineering activities, including operational security assessments and renewal of system ATO.	**Primary**: measure frequency of ATO/security renewals. **Secondary:** use scaled analogy data from prior program to estimate cyber engineering team size.

WBS 2.2 – Security Operations Center Support

- Represents efforts required to support Security Operations Center (SOC) activities
- Includes monitoring, incident support, vulnerability assessment, and related efforts

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Stand-up of program SOC support for proactive (monitoring and assessment of potential threats) and reactive (incident response and recovery) functions.	**Primary**: number of incidents and/or support tickets from analogous program. **Secondary**: number of system users
Case Study 2 	Likely few changes unless authentication management creates additional scope.	**Primary**: collect cost drivers used by enterprise SOC (i.e., users, servers, and/or T-shirt sizing) and adjust charge if needed. **Secondary**: scaled analogy from other systems that completed ZTA update to determine amount of labor needed.

WBS 2.3 – Security Software Maintenance

- Represents annual maintenance and license renewals associated with items purchased or maintained by system
- Should include all license purchased in WBS 1.4 (Secure Software Procurement) along with pre-existing security software COTS licenses

Case Study	Relevant Program Activities	Proposed Estimating Methodology
Case Study 1 	Annual maintenance of any COTS products purchased in "Secure Software Procurement" category.	**Primary**: leverage Cost-per-License metrics used in Secure Software Procurement, with applicable renewal costs in place of procurement. **Secondary**: number of system users
Case Study 2 	Include any additional COTS license purchases in assumptions for annual sustainment and subscription fees.	**Primary**: leverage Cost-per-License metrics used in Secure Software Procurement, with applicable renewal costs in place of procurement. **Secondary**: number of system users

Limitations

- Lack of historical data for emerging security efforts (namely Zero Trust and Secure by Design)
- Cyber engineering/assessment may prove particularly hard to quantify and estimate in early stages
- Cybersecurity is rapidly evolving, and a WBS will require constant updates to stay current
- Scope confined to information systems, more customization would be needed for systems with embedded hardware or other specialized applications

Conclusions and Next Steps

- Secure Software WBS developed to de-mystify cybersecurity landscape and standardize how estimators track cyber costs
- Future research should build on common structure to collect data and generate CERs
- Future research should also consider application to specialized systems beyond information systems

Questions/Answers