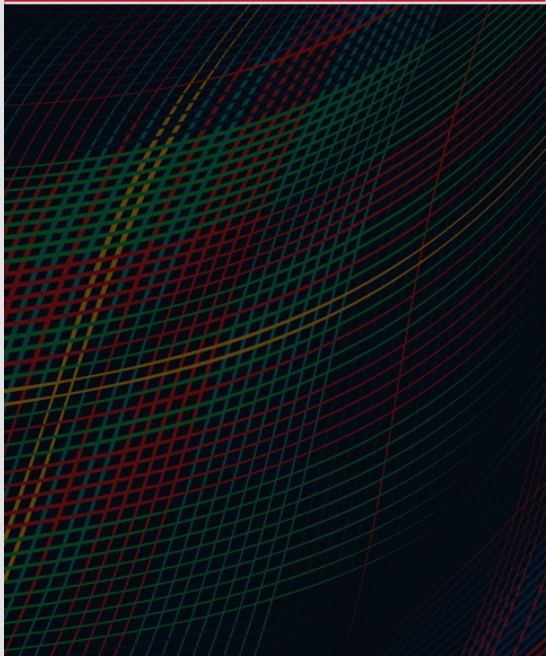
Carnegie Mellon University
Software Engineering Institute

Can a Cybersecurity Parametric Cost Model be Developed?

Current State of Practice and a Few Ideas

SEPTEMBER 2024

Anandi Hira
Christopher Miller



Document Markings

The following markings MUST be included in work product when attached to this form and when it is published.

For purposes of double anonymous peer review, markings may be temporarily omitted to ensure anonymity of the author(s).

DM24-1141

Topics

- Need for a Cybersecurity Parametric model
- Baselining Cybersecurity
- State of the Practice Summary
- Cybersecurity Parametric Model Conceptual Overview
- Conceptual Cybersecurity Parametric Model
- Data for Model Creation and Calibration
- Data for Model Usage
- A Few Ideas and Lingering Thoughts

Need for a Cybersecurity Parametric Model

Carnegie Mellon University Software Engineering Institute

Every Department of Defense (DoD) program needs to account for, credibly estimate, budget/plan, and assess the performance of their cybersecurity activities.

- Cost estimators and program planners need to determine how much new (or more stringent) cybersecurity requirements are going to impact their independent cost estimate (ICE) associated with a request for proposal (RFP) and their subsequent ability to evaluate proposals.
- Cost estimators and program planners need to provide defensible Basis of Estimates (BoEs) – justifications for cost estimates of activities.
- Chief engineers, directors of engineering, and security officers need to identify and recruit a cybersecurity workforce adequate in both talent and skill to meet their staffing requirements.
- Program managers require sufficient insight into cybersecurity performance to quantitatively plan, evaluate alternative courses of action (COAs), and manage their activities during program execution.

Creating and propagating a cybersecurity parametric model would allow them to

- reliably estimate the effort and cost of individual cybersecurity activities
- estimate a tailored set of cybersecurity activities to obtain an overall cybersecurity cost for a program
- obtain a defined and normalized set of cybersecurity data

Tecolote Research Inc.:
"Cybersecurity costs are becoming more of an issue across all programs"

Air Force Enterprise IT & Cyber Infrastructure Division
Cybersecurity broken out as separate WBS element in MIL-STD-881.
"Very intriguing area and most definitely an area for cost growth."
"We try to track these costs… as they seem to be increasing cost drivers."

Technomics (MacDougall et al., 2024)
"Programs eagerly seek to understand the cost to modernize their cybersecurity posture but lack the data to estimate cost properly."

Naval Sea System Command (NAVSEA)
Built a cost tool to meet 2 primary needs:
1. Ensure all tasking was accounted for when developing costs.
2. Provide cost transparency to all customers.

Baselining Cybersecurity

First step is to estimating any activity is to lock down its definition in terms of the scope and work to be performed:

- work breakdown structure (WBS) (granularity balanced with data availability)
- work products (e.g., authorization to operate [ATO] packages)

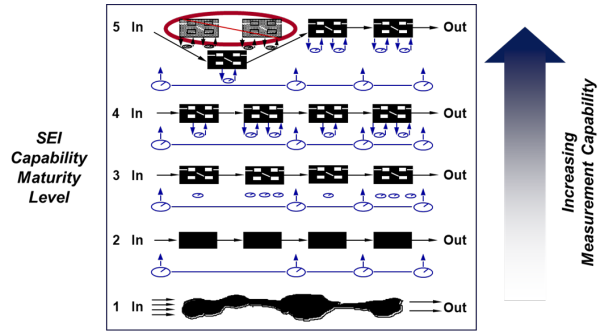
This research leveraged the following two documents to serve as a generic cybersecurity WBS:

- Alberts, Christopher et al. *Acquisition Security Framework (ASF): Managing Systems Cybersecurity Risk (Expanded Set of Practices).* CMU/SEI-2023-TN-004. Software Engineering Institute (SEI), Carnegie Mellon University (CMU). October 2023.
- MacDougall, Austin; Gellatly, William; & Kleinman, Jessica. *Advancing the Art of Cyber Cost Estimating*. International Cost Estimating & Analysis Association (ICEAA) Professional Development & Training Workshop. May 2024.

State of the Practice Summary

Literature review and industry outreach activities confirmed that cybersecurity effort is

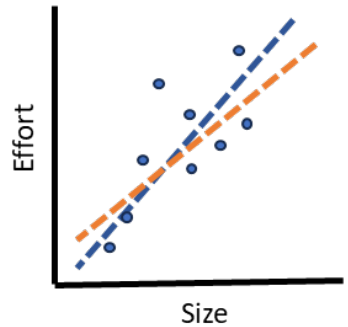
- estimated by determining the level of effort/headcount over time
- typically not a separate line item (i.e., effort is tracked as part of a larger task element)



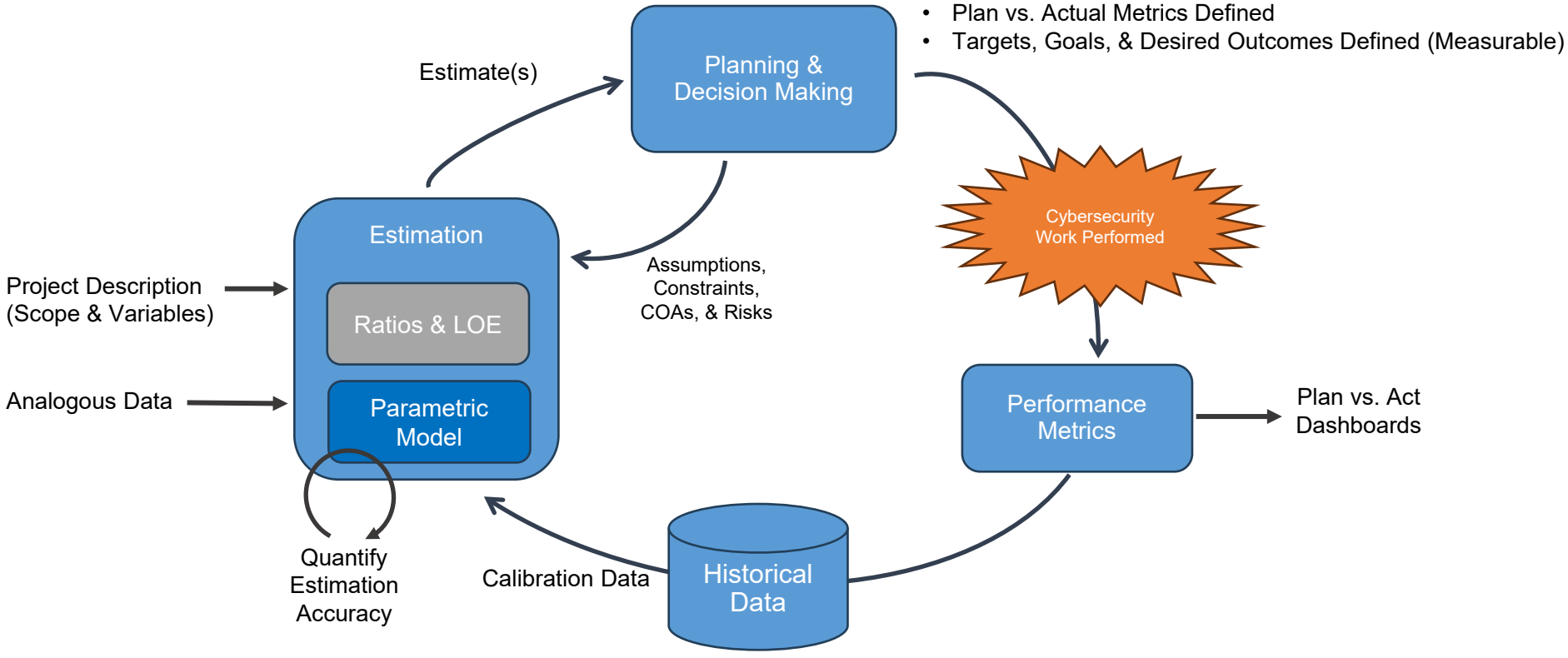
Paulk et. al., The Capability Maturity Model: Guidelines for Improving the Software Process

Parametric Modeling Principles

- Parametric models represent the results of conducting regression and correlation analysis on large sets of historical data from completed projects.
- Parametric models include many variables that have been quantitatively proven to affect cost (i.e., cost drivers).



Cybersecurity Parametric Model Conceptual Overview



Cybersecurity Parametric Modeling Approaches

Carnegie Mellon University Software Engineering Institute

Model Extension

- Leverage existing parametric models and extend their scope to account for cybersecurity.

Product Focused

- Select a few key cybersecurity products (e.g., program protection plans [PPPs] and ATO packages) to target data collection and create cost estimates for individual work product and cybersecurity-focused deliverables.

Activity Driven

- Leverage existing cybersecurity guidance to bound the scope and collect data (subjective and objective).

Cybersecurity Parametric Modeling Comparisons

Carnegie Mellon University Software Engineering Institute

Option	Stand-Up Effort	Inputs & Calibration	Outputs & Information
Model Extension	• The least stand-up effort is required. • Leveraging existing parametric models accelerates the time to build a model.	• Subject data (subject matter expert [SME] input) about cost driver impact could enable creating a parametric model quickly. • Data would need to be collected to validate the model prior to use.	• How much effort and cost are associated with cybersecurity? • How much cost is added by increasing cybersecurity practices?
Product Focused	• A moderate amount of stand-up effort is required. • Focusing on a few key products helps limit the impact of data collection.	• Selecting key products (and collecting related data) is required. • Descriptive statistics depend on all collecting sufficient data points to achieve statistical validity.	• What effort and cost are required to put together an ATO package? • What effort and cost are associated with developing a PPP?
Activity Driven	• Significant stand-up effort is required. • It requires significant effort to collect data for all the activities included in a cybersecurity WBS.	• Identification and data specifications for each activity, data collection, verification, and storage (until sufficient data is accumulated) are required. • Standard operating procedure (SOP) summaries indicate that this data may not organically exist (i.e., limited to subjective data).	• How much effort and cost are estimated for individual cybersecurity activities? • How much effort and cost are estimated to perform a tailored set of cybersecurity activities?

Conceptual Cybersecurity Parametric Model

Indicator and Interpretation

Estimate of Cybersecurity Costs (Information Need)
Study Result: Developing a parametric model for estimating cybersecurity is feasible. Granularity and fidelity of the model depend on the quality of subjective and objective data as well as the uniformity of cybersecurity activities (historical and future).

Analysis Model

Description of System/Software

Description of Cybersecurity (to Be Estimated)

Cybersecurity Parametric Model

SE/SW Effort

Cyber Cost Drivers

Cyber WBS/Practices

Generate Estimates

Derived Measures

SE/SW Effort Estimates

Cost Drivers (Calibrated)

Measurement Function

Refinement of Cost Drivers (Expert Judgement)

Validation of Cost Drivers (with Historical)

Base Measures

Effort Estimates for Individual and Overall Cybersecurity Activities

Descriptive Statistics for Individual and Overall Cybersecurity Activities

Measurement Methods

Interviews/ Workshops

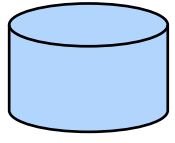
Data Calls/Data Mining

Entities & Attributes

Cybersecurity Experience

Cybersecurity Data

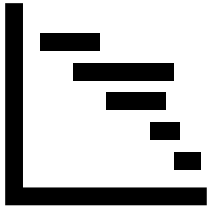
SMEs



Historical Data

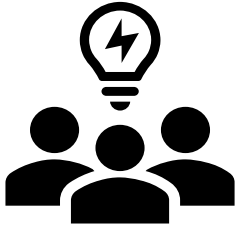
- System/SW Information
- Modeling Activity
- Modeling Artifact

Data for Model Creation and Calibration



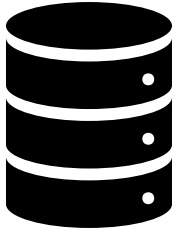
Project's Information/Description

- Domain, platform, and scope (i.e., mix of organic and contractor)
- Systems engineering and software engineering (activities and effort)
- Cybersecurity activities and work products



Experiential Data (Subjective)

- Collected from SMEs using informal and formal data collection methods



Historical Data (Objective)

- Data collected from the results of performing cybersecurity activities and/or creating cybersecurity work products (i.e., PPP); data may be
  - industry/organization
  - local/project

Data for Model

Inputs (Independent Variables and Cost Drivers)

- SE/SW effort is known or estimable.
- Cybersecurity activities have been defined.

Outputs (Dependent Variables)

- Cybersecurity effort by WBS activity and/or work product is measured.

Assumptions

- Cybersecurity effort is a percentage of systems engineering (SE) effort (Constructive Systems Engineering Cost Model [COSYSMO]) and/or software (SW) development effort (Constructive Cost Model [COCOMO]).
- LOR cost drivers can accurately account for differences (and be reliably adjusted).

A Few Ideas and Lingering Thoughts

- In a DoD system life cycle, cybersecurity activities evolve as the system matures. Estimation of cybersecurity may be better approached based on the life cycle phase.
  - Earlier phases: focus on cost to 'baking in cyber'
  - Later phases: focus on cost of 'maintaining a secure system'
- Start small and local.
  - Develop an approach based on specific purpose; consider data availability and staff knowledge/skills.
- Measure (and acknowledge) your estimation prediction accuracy.
  - If not overtly stated, users falsely assume precision and accuracy.

"It is dangerous to make forecasts, especially about the future"
– largely attributed to Mark Twain, others cite Yogi Berra

Contact for More Information

Dr. Anandi Hira
Data Scientist

Email: avhira@sei.cmu.edu

Dr. Christopher Miller
Member of the Technical Staff, Engineer

Email: clmiller@sei.cmu.edu

Join our team!

We are looking to grow our team and add a member who has these skills:

- software estimation, process modeling, and software measurement
- able to serve as an analytical, customer-focused expert who works with customers
- familiar with parametric cost models.

If this opportunity sounds interesting, read more about it or scan the QR code on the left.