RSA 2022

How Much is Good Enough?

Measuring the Complexity of Cyber Environments

Brett Tucker, PMP, CSSBB, CISSP, CAP

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

DM22-0471

RSA 2022

How Much is Good Enough?

Measuring the Complexity of Cyber Environments

Brett Tucker, PMP, CSSBB, CISSP, CAP

Value Proposition in Understanding Complexity

Organizations must strive to make risk-based decisions to optimize their security stack.

- This is not as easy as it sounds.

Enemy tactics and techniques continually shift as much as the technology is evolving.

- Security stacks are diverse and complex.

The **complexity of the system may inhibit or enhance performance**.

- **Measurement would enable better decisions.**

Can Complexity of Cyber Be Measured?

Complexity – Cambridge Dictionary defines as the state of having many parts and being difficult to understand

- This research focuses upon complexity of cybersecurity that inhibits strategic objectives at the organizational level.

HYPOTHESIS:

- System complexity is measured on a spectrum that ranges from overly simplistic to burdensome with a middle range of optimal performance.
  - For example, a system may have so much complexity that the performance is hindered, and organizational objectives are impacted in a negative sense.
  - Alternatively, the system complexity may be minimal and allow threat actors to find the system far easier to navigate and exploit in a shorter time period resulting in greater negative impact.
  - The optimal range of complexity strikes a balance between the ends of this spectrum where the system operates efficiently, yet threat actors have trouble navigating it once within boundaries.

Decomposing Cybersecurity Complexity

The cybersecurity stack of any organization has many diverse elements.

These elements may be contributing in part or in tandem to create a complex ecosystem.

An optimal balance is necessary to deliver value to the organization.

Quantifying System Interfaces

Complexity may be related to the number of interconnections in a system.

- Technical or even administrative

Think of trying to find agreement upon a single issue among all conference attendees.

- Communication paths alone can be complex

May be quantified for the index using Metcalfe's Law

- Communication Channels = N^2
- Where N = number of nodes in the system
- Weighting of nodes may be considered based upon critical nature

Quantifying Organizational Capability

Organizational Capability

Complexity may be related to the ability of the organization to manage and utilize its assets effectively.

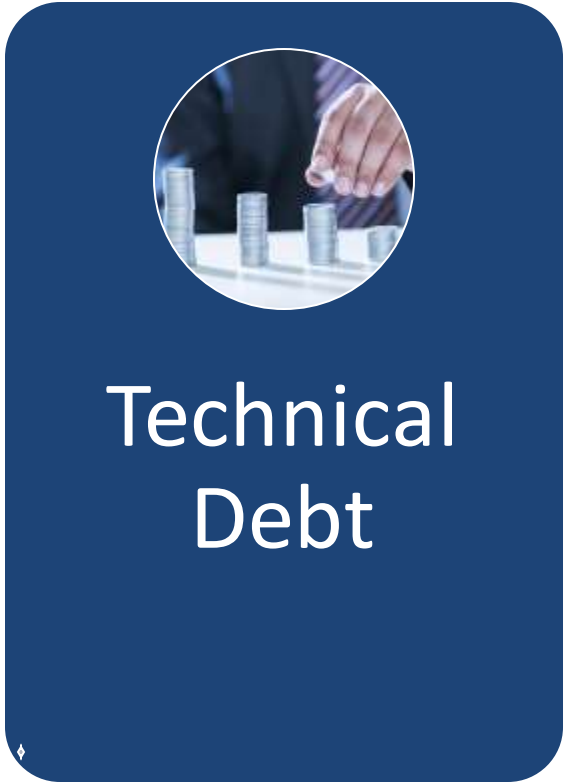
- Represented by workforce skills and capabilities

This complexity factor may be measured by analyzing the structure of the organization and needs as they relate to the security stack.

- National Initiative for Cybersecurity Education (NICE) The National Cybersecurity Workforce Framework Version 1.0
- *Structuring the Chief Information Security Officer Organization*

Scores may be determined by organizational needs.

Quantifying Technical Debt



Complexity may also depend upon technical debt.

- Errors in the code base
- Architectural inadequacies
- Legacy infrastructure

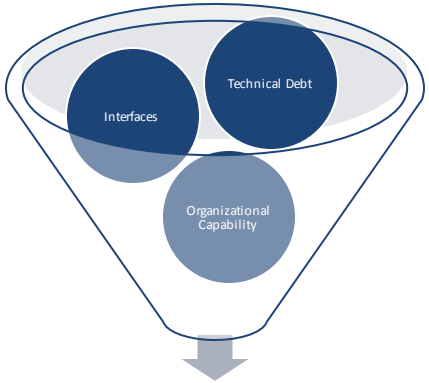
Some research shows that the following may be considered for quantification:

- Heuristics related to errors per lines of code
- Historic customer support costs may provide some additional insights

Index Will Come from an Integration of Parts

The three elements will each yield a quantitative measure.

- **Additional research needed** to determine the validity of the math.
- **Data sets or model systems must be identified** or built to validate the complexity index model.
- Other elements may be identified as the model evolves.
- **Weighting factors** may be a significant consideration as understanding evolves.



Complexity Index

$$S_i = \sum_{j=1}^{n} S_{ij} W_j$$

- $S_i = Complexity\ Index\ for$ "i" elements
- $S_{ij} = the\ score\ of\ the\ ith\ element\ on\ the\ jth\ criterion$
- $W_j = the\ weight\ of\ the\ jth\ criterion$

Contact Information

Brett A. Tucker, PMP, CSSBB, CISSP, CAP

Technical Manager,

Cyber Risk Management

CERT Division

Software Engineering Institute