Striking the Balance:

Measuring and Managing 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.

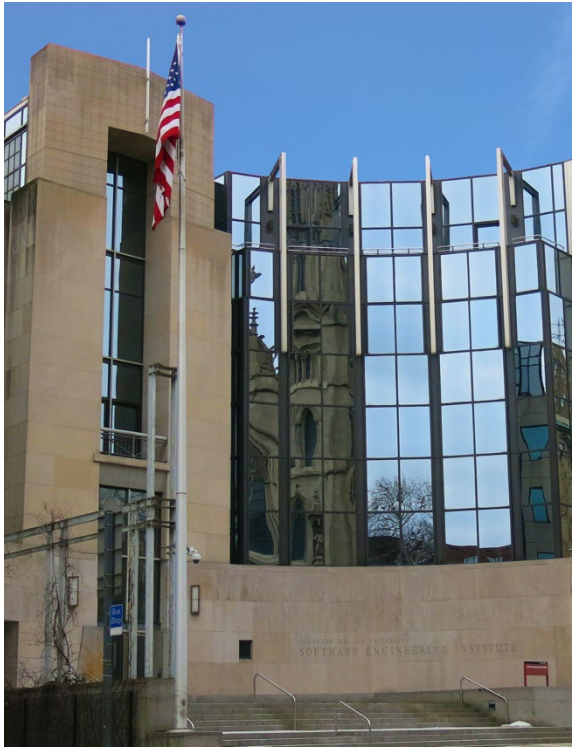
DM22-0471

Carnegie Mellon University (CMU)

Pioneering discoveries that enrich the lives of people on a global scale

- Turning disruptive ideas into success through leading-edge research
- 2021 *U.S. News and World Report* rankings:
  - #1 in computer engineering, AI, cybersecurity, and software engineering
  - #2 in overall computer science
  - #3 in data analytics/science

CMU Software Engineering Institute (SEI)



Bringing innovation to the U.S. government

- A Federally Funded Research and Development Center (FFRDC) chartered in 1984 and sponsored by the DoD
- Leader in researching complex software engineering, cyber security, and artificial intelligence (AI) engineering solutions
- Critical to the U.S. government's ability to acquire, develop, operate, and sustain software systems that are innovative, affordable, trustworthy, and enduring

The CERT Division: Birthplace of Cybersecurity

Trusted
Conducting research for the U.S. Government in a non-profit, public-private partnership

Valued
Collaborating with military, industry, and academia globally to innovate solutions

Relevant
Achieving technology and talent results for our mission partners

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.

Threat actor 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.**

Use Case Example – Why Measure Complexity?

Imagine having a speedometer for your cybersecurity control stack.

- Provides indication of activity of your system.
- Could be thought of as a proxy for risk.
  - High speed = high risk
  - Low speed = high risk

Changes to assets and controls could impact the index.

- Think about physical, administrative, and technical controls.
- Dynamic environments that have many devices coming and going.

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 negatively.
  - Alternatively, the system complexity may be minimal and allow threat actors to navigate and exploit the system 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 its 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.

Additional Elements to Consider

Other elements may be considered in this model.

However, these elements may be “cross-cutting”.

Cross cutting considerations include:

- **Supply Chain**
- **Resource Constraints**

Quantifying System Interfaces

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

- Technical or even administrative

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

Technically speaking, net flow may provide measure.

- Sensor selection and placement critical
- May only consider internal flow

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
- Process efficiencies may also be considered here

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.

- Size and potential errors in the code base
- Architectural inadequacies
- Legacy infrastructure

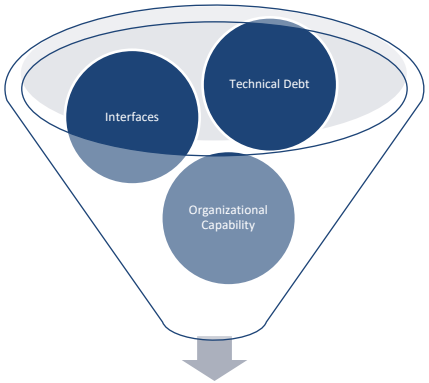
Some research shows that the following may be considered for quantification:

- 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