Quantifying Cross Sector Cyber Performance Goals (CPGs)

Brett Tucker, PMP, CSSBB, CISSP, CGRC

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

DM23-0619

CISA CPGs Promise to Deliver

The community is excited about CPG application in terms of:

- Establishing baseline practices to reduce risk exposure
- Benchmarking for improved maturity
- Prioritizing security practices
- May lead to a greater understanding of aggregate risk to the nation

Challenges for community acceptance may include:

- Currently voluntary
- **Estimates of cost, complexity, and impact provided**
- Approaches for quantification may vary based on context

Quantification Raises Confidence

Quantification of **cost, complexity, and impact** would make the CPG framework more robust

- Of the **36 sub-elements distributed over the 7 process areas**, a uniform standard of measurement would provide:
  - Consistent basis for analysis
  - Equivalent comparison that enables prioritization of resources

Possible approach:

1. **Define** each metric explicitly to include means of measurement
2. **Establish a scoring scheme** that aligns measures with current scale
3. **Benchmark** scoring with existing industry best practices
4. Periodically refine and **update** scores with evolution of TTPs and technology

Quantification Raises Confidence (continued)

Cost

- Survey of commercial off the shelf tools, cybersecurity professional average salaries, and other related factors would provide quantified ranges of control costs
  - Total cost that spans the life of the control should be considered to enable organizational asset planning and management
- Improved cost estimates may inform procurement planning and prioritization

Cost Approach Use Case Example

Define – "COST" score shall include initial investment in procurement, install, and training

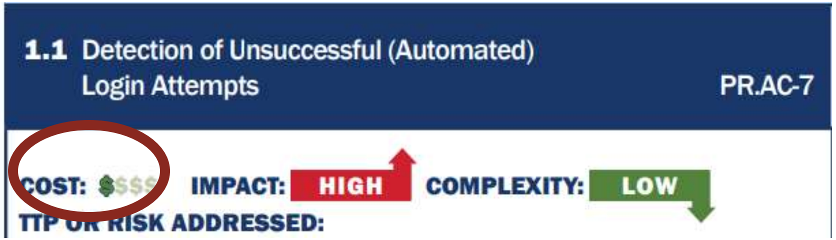
Establish Scoring Scheme – notional tolerance bands could include

- $ = less than $100K
- $$ = $100K - $1M
- $$$ = $1M - $10M
- $$$$ = greater than $10M

These values may scale to context of the organization.

Benchmark – survey top three off the shelf solutions across at least three sectors

Update – periodic updates plus specific circumstances that would require update



1.1 Detection of Unsuccessful (Automated) Login Attempts PR.AC-7

COST: $$$$ **IMPACT:** HIGH **COMPLEXITY:** LOW

TTP OR RISK ADDRESSED:

Quantification Raises Confidence (continued)

Impacts

- Several frameworks and methodologies exist for quantifying risk impacts, yet few help with control efficacy
- For the CPG framework, the goal would involve a survey of most risk incidents to determine potential efficacy of practice suggested
- Must consider primary impacts as well as secondary
  - Various response strategies suggested by the CPGs may overlap or amplify each other
  - For example, 7.2 Incident Response Plans may be enhanced with 4.3 and 4..4 Cybersecurity Training

Impact Approach Use Case Example

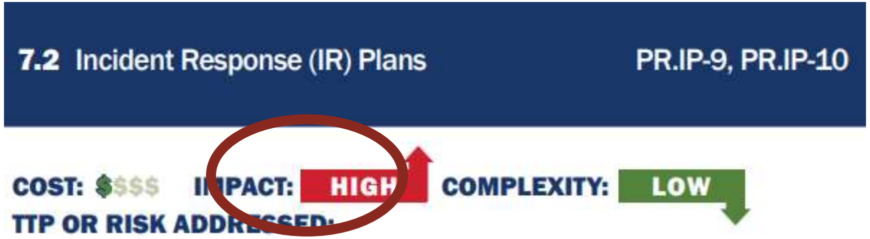
Define – “IMPACT” score includes consideration of control effect compared to potential loss

Establish Scoring Scheme – notional tolerance bands could include

- High – No more than 4 hours of operational downtime per year
- Medium – Between 4 – 24 hours of downtime per year
- Low – Greater than 24 hours of downtime despite practice in place

Benchmark – survey of sector SOCs for downtime despite practice in place

Update – periodic updates plus specific circumstances that would require update



7.2 Incident Response (IR) Plans PR.IP-9, PR.IP-10

COST: $$$$ IMPACT: HIGH COMPLEXITY: LOW

TTP OR RISK ADDRESSED:

Quantification Raises Confidence (continued)

Complexity

- Maya be based on several fundamental pillars
- **NOTE:** not all may be applicable in the CPG context
  - Network traffic
  - Organizational Capability
  - Technical Debt
  - Supply Chain and Third-Party Providers
  - Resources
- Complexity may inform upon implementation and usage challenges

Complexity Approach Use Case Example

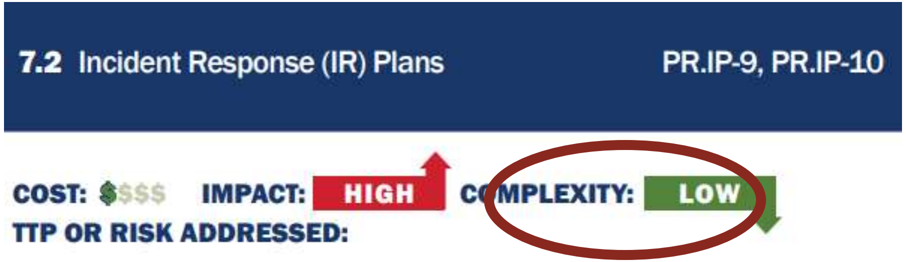
Define – “COMPLEXITY” score includes consideration of system burden despite practice implementation, ease of implementation, and potential for errors (e.g., Tech debt, configuration, etc.)

Establish Scoring Scheme – notional tolerance bands could include

- High – Implementation could take up to a year or more
- Medium – Implementation could take up to 6 months to a year
- Low – Less than 6 months to implement

Benchmark – compare with other analogous system implementation efforts

Update – periodic updates plus specific circumstances that would require update



7.2 Incident Response (IR) Plans PR.IP-9, PR.IP-10

COST: $$$$ IMPACT: HIGH COMPLEXITY: LOW

TTP OR RISK ADDRESSED:

Contact Information

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

Technical Manager,

Cyber Risk Management

CERT Division

Software Engineering Institute