Managing Risk:
Capturing Full-Value of Cybersecurity Guidelines

Nazli Choucri
Professor of Political Science
nchoucri@mit.edu

Gaurav Agarwal
Research Affiliate, MIT Political Science
gauravag@mit.edu

The Problem

Guidelines Harbour Both Risks & Opportunity Costs

1 Policy and guidelines are routinely transmitted in text form.
- Difficult to integrate or understand the policy-technology links.
- Obscures risks inherent in policy.

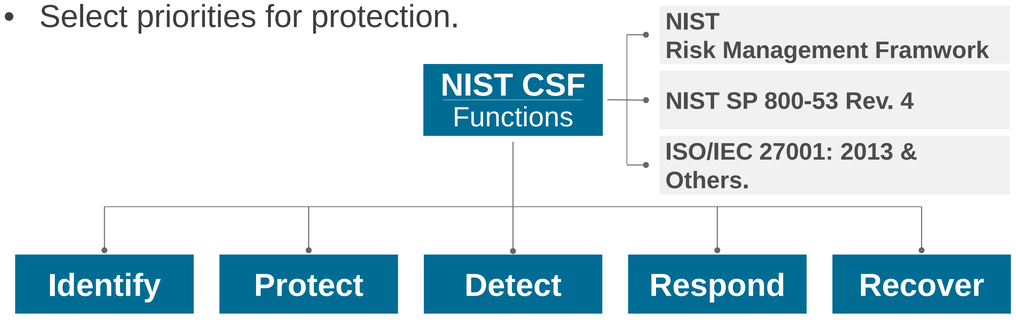
2 Text form contains critical knowledge obscured by syntax.
- Prevents locating interactions, feedbacks, special views, etc..
- Inhibits dynamic understanding of system cybersecurity.

3 Information on risk potential is embedded deep in text format.
- Impedes managers, security experts, and policy analysts.
- Impediment undermine the effectiveness of guidelines etc.

Value to Enterprise – Business & Industry

Support Cyber Risk Management in NIST Cyber Security Framework version 1.1.

- Customize tools to identify risk.
- Capability maturity to handle risk based on NIST CSF and other guideline texts.
- Strengthen early warning system.
- Select priorities for protection.



Analytics for Capability Maturity

Multi-method Analysis of Cybersecurity Guidelines

1 Define Policy Domain for Risk Analysis	2 Create model of system & information Flows	3 Construct Network of Dependencies & Risk Zones	4 Drill-Down for Detailed Targeted Analysis	5 Identify Risk Properties to Assess System Impact
1.Select texts. 2.Formalize rules to extract data	1.Create dependency structure matrix (DSM). 2.Cluster & partition DSM to reveal “hidden features”.	1.Analyze networks of information flows 2.Identify critical control points & human vs. technical operations.	1.Provide tools for on demand analysis 2.Test system for risk and resilience.	1.Formalize risk properties. 2.Assess system-wide and other impacts.

Consistent with Science of Security – Hard Problems*

The Five Hard Problems

* See https://www.nsa.gov/what-we-do/research/science-of-security/

Resilient Architectures	Scalability & Composability	Policy Governed Secure Collaboration	Security-Metrics-Driven Evaluation	Understanding & Accounting for Human Behaviour

Proof of Concept: Cybersecurity of Aviation Energy Systems

Airport Energy Service Interface is Central to Aviation System

- Smart grid is central to power systems.
- NIST provides guidelines for smart grid cybersecurity.

NIST Guidelines Converted to Structured Model

- Model provides data to generate graph views.
- Views identify critical nodes for system security.
- Nodes signal potential vulnerabilities.
- Vulnerabilities identify risk and impact on security.

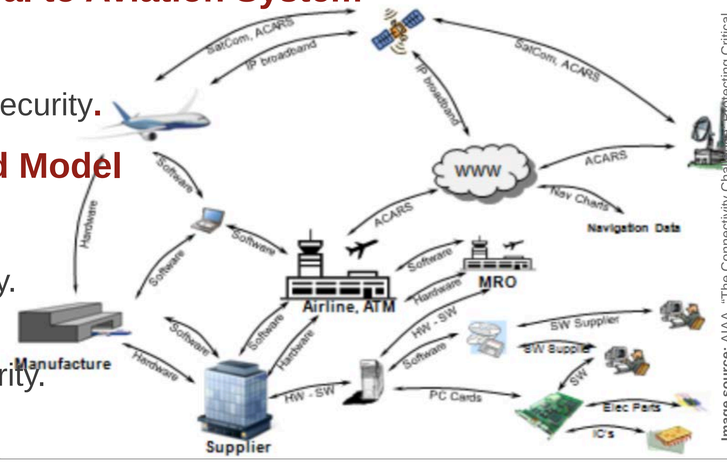


Image source: AIAA, “The Connectivity Challenge: Protecting Critical Assets in a Networked World: A Framework for Aviation Cybersecurity”, An AIAA Decision Paper, August 2013.

