# A Framework for Open Science Cybersecurity Programs

Bob Cowles, Kay Avila, Craig Jackson
Trusted CI - NSF Cybersecurity Center of Excellence

HEPiX Fall Workshop, Barcelona
10 - 10 - 2018

# Trusted CI Mission Statement

Trusted CI's mission is to provide the NSF community a coherent understanding of cybersecurity's role in producing trustworthy science and the information and know-how required to achieve and maintain effective cybersecurity programs.

This document/presentation is a product of the Trusted CI. Trusted CI is supported by the National Science Foundation under Grant ACI-1547272. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation.

# Background

## Guide version 1 published in August 2014

- 46 pages of text (tl:dr?) and numerous templates
- There have been plans for several years for an update
  - Other priorities *e. g.,* Large Facilities Manual, Community Survey
  - Rapidly evolving goals and requirements

## Guide version 2 planned for January 2019

- During early planning and after experience in training sessions, surveys, etc. we realized the need for a framework for **Programs** (not just controls) that addressed the variability in the community
- The framework would address **cybersecurity program** requirements
- We need community involvement for the effort

## Framework v0.9 in January 2019; v1.0 in March 2019

# Framework Design Goals

- **Scalable:** make it easy for smaller and newer projects/facilities to navigate and make use of the framework and its resources.
- **Template and resource review/revision:** Tighten the relationship between framework and the templates and other resources.
- **Tools:** Document self-evaluation tools for projects to rate themselves
- **Training:** Update training used for the Summit and other venues
- **Metrics:** Design to provide a measurement of community use.
- **Accessibility/usability:** Lower barriers for adoption.
- **Prioritized controls:** Phased implementation of basic controls first
- **Community engagement:** Significant interaction with organizations in the US and internationally.

# Using the Framework as a Starting Point

Most compliance frameworks don't prioritize and end up being overwhelming with hundreds of pages of reading material and checklists that seemingly go on forever

This Framework will aid ANY project/facility wishing to establish a cybersecurity program and provides prioritized, easy-to-read requirements for the first steps to the more difficult frameworks

# Information Security Practice Principles*

**Comprehensivity** *("Am I covering all of my bases?")*

**Opportunity** *("Am I taking advantage of my environment?")*

**Rigor** *("What is correct behavior, and how am I ensuring it?")*

**Minimization** *("Can this be a smaller target?")*

**Compartmentation** *("Is this made of distinct parts with limited interactions?")*

**Fault Tolerance** *("What happens if this fails?")*

**Proportionality** *("Is this worth it?")*

*https://cacr.iu.edu/principles/ispp.php

# Using the Principles as Goals for Open Science Cybersecurity Programs

**Comprehensivity** - Cover mission requirements

**Opportunity** - Take advantage of host institution environment

**Rigor** - Implement evidence-based controls

**Minimization** - Limit and eliminate unnecessary complexity

**Compartmentation** - Separate systems and data by classification level

**Fault tolerance** - Plan for incidents and detection, response, recovery

**Proportionality** - Accept risks that don't endanger the mission

# AFCEA's The Economics of Cybersecurity

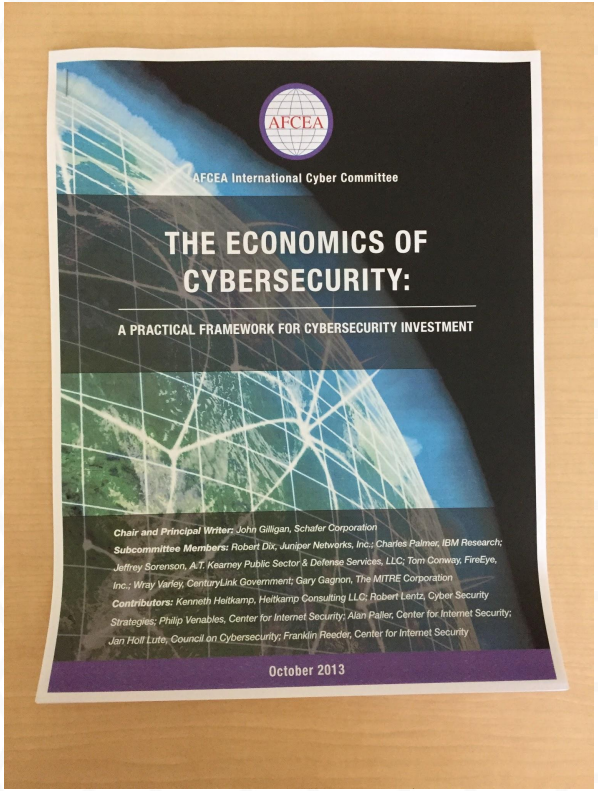
## John Gilligan, fmr USAF CIO

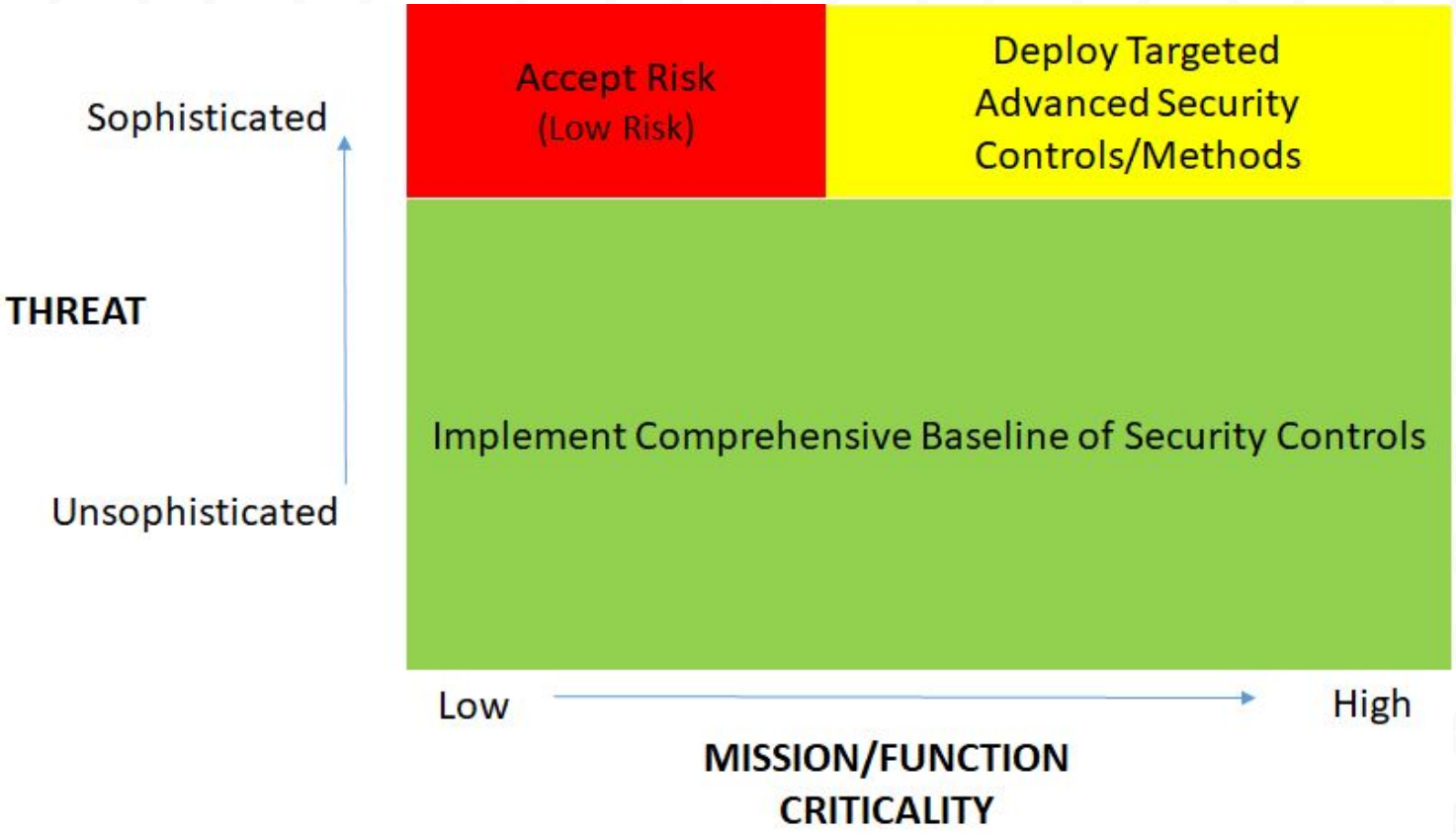
Background

- Cyber has limited data for quantitative assessments.
- Most cyber-attacks are unsophisticated.
- Total protection is uneconomical.

Takeaways:

- Focus on low-cost, high-impact interventions.
- Prioritize defenses against common, unsophisticated attacks.
- Utilize targeted defenses against high-sophistication, high-criticality attacks.
- Accept risk of high-sophistication, low-criticality attacks.



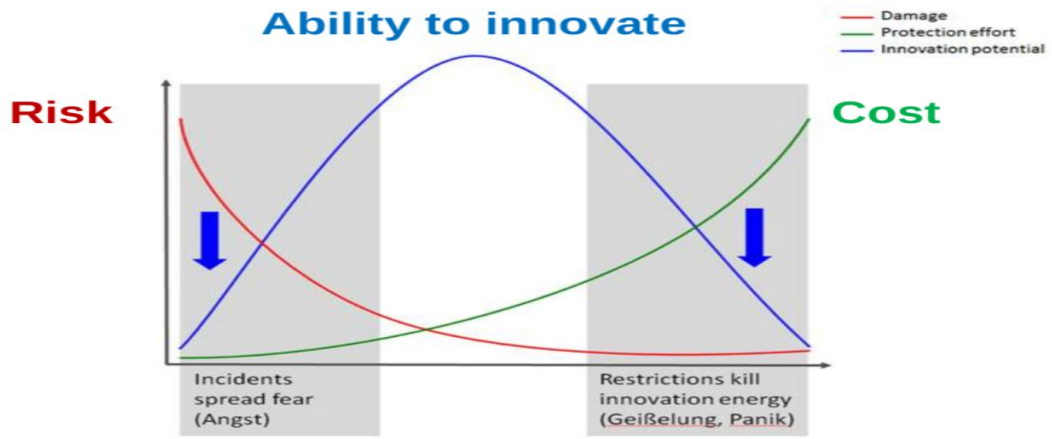

Accept Risk
(Low Risk)
Deploy Targeted
Advanced Security
Controls/Methods
Sophisticated
THREAT
Unsophisticated
Implement Comprehensive Baseline of Security Controls
Low
High
MISSION/FUNCTION
CRITICALITY

# Provide Guardrails, not Barriers

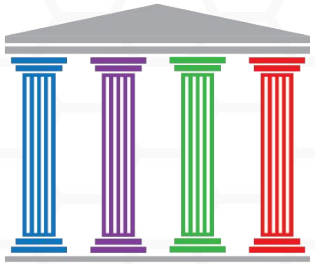
SIEMENS

**Economic Trade-off:**
**Relationship between risk, cost and ability to innovate**

Too little and too strong security governance are hindering innovation



# Framework Pillars



## Mission Alignment

Information classification, asset inventory, external requirements

## Governance

Roles and responsibilities, policies, risk acceptance, program evaluation

## Resources

People, budgets, services and tools

## Controls

Procedural, technical, administrative safeguards and countermeasures

# Framework Web Design (draft)

Landing page contains:

- (patterned after https://www.cisecurity.org/controls/ )
- Clickable links to short descriptions (about one page)
  - Context
  - Requirements
- Link to expanded document (about 15 pages)
- Link to the updated templates
- Links to Special Topics
- Links to recommended reading references
- Links to curated references

# https://trustedci.org/framework (draft!!!)

## Summary sections

- Foundation
- Pillar: Mission Alignment
- Pillar: Governance
- Pillar: Resources
- Pillar: Controls
- Operations

## Special Topics (SCADA, *etc.*)

## Access the Framework

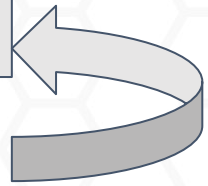
## Access the Templates

## Primary resources

- Principles …
- AFCEA
- Other Primary docs
- …

## Recommended reading

- Curated resources



The Framework

# Plan

November 2018 -
- Initial draft for comment (some revised templates)

January 2019 -
- Version 0.9 for comment

March 2019 -
- Version 1.0 published

Ongoing
- Maintenance - updates and revisions

# Community Involvement (possible options)

Trusted CI Advisory Board
NSF Large Facilities Security Team
HEPiX (you)
WISE SCI and Sirtifi
DoE (ESNET), other DoE open science labs
Campus Champions
CASC (Coalition for Academic Scientific Computation)
…
others?

# Questions?

bob.cowles@gmail.com