Beyond the Beltway

The Problems with NIST's Approaches to Cybersecurity and Alternatives for NSF Science

Craig Jackson, Chief Policy Analyst
Bob Cowles, Senior Fellow
Scott Russell, Senior Policy Analyst
cacr.iu.edu

August 2017
2017 NSF Cybersecurity Summit

CENTER FOR APPLIED CYBERSECURITY RESEARCH
INDIANA UNIVERSITY
Pervasive Technology Institute

http://hdl.handle.net/2022/21732

Outline

1. Context
2. The Problems with NIST's Approaches to Cybersecurity
3. Healthier Alternatives
4. Your Summer Reading List

Context

The Role of Cybersecurity Frameworks & Control Sets

Pillars of a Cybersecurity program

- GOVERNANCE *Roles, Processes, Policies*
- RESOURCES *People, Infrastructure, and Security Tools… Money*
- CONTROLS *Procedural, technical, administrative safeguards/countermeasures*

Bottom Line:

Competent security programs require adopting some resources and tools to support program development, maintenance, and optimization.

What to select? Why to select?

Effective.

Inclusive. Evidence-based. Adaptable.

Efficient.

Doable. Affordable. Prioritized. Time-saving.

This community requires both.

Problems

Is risk management really a good fit for cybersecurity?

1. Risk management processes found in the existing frameworks (NIST RMF; NIST CSF) make questionable assumptions:
   a. Cybersecurity presents a measurable environment with some historical stability (e.g., actuarial history).
   b. Organizations have the time, money, and expertise to execute intensive procedural regimes.
2. As a result:
   a. Much time and money has been wasted on quasi-quantitative risk assessments with little or no validity…
   b. Rather than getting the basic processes and protections in place frameworks like NIST RMF give lip service to risk management, but devolve into massive documentation games and checklist maintenance.

NIST RMF has been looming...

NIST RMF was created in response to the Federal Information Security Management Act of 2002 (FISMA), to create information security standards for the federal government. FISMA set out the basic process, and NIST was tasked with fleshing out the details. The detailed approach created by NIST is generalized as the Risk Management Framework (RMF).

In last year's plenary session, the United States Antarctic Program's Tim Howard appeared to make the case that NIST RMF and SP 800-53 are obvious sources of procedural and control selection guidance for the NSF science community.

Yet, Anurag Shankar and Susan Ramsey told a harrowing story of RMF in application.

NIST Risk Management Framework (RMF)

Efficient?... Heck no!

1. Assumes you have a lot of time, money, and expertise to devote to cybersecurity compliance. (And, we can't clone Anurag.)
2. Massive control list and incredible amounts of documentation.
3. Not prioritized. Kitchen sink approach. Regardless of assessed risk level, you will have a LOT of controls to implement that are all treated equally.
4. Costly to interpret into system engineering requirements. Hundreds of pages of controls can turn into thousands of pages of requirements.
5. Distracts from mission and security.

   The SANS 2016 IT Security Spending Trends Survey reported regulatory compliance as a much more significant driver for spending than, e.g., reducing attack surface, improving visibility (detection), new, advanced threats and techniques, and improving incident response. It is possible to have a lightweight compliance regime, but that is NOT what we have in with NIST RMF.

NIST Risk Management Framework (RMF)
Effective?... It's costly, but does it get us security?

Facial Problems w/ RMF and 800-53:

1. Vagueness. Written in abstractions that are difficult to test for adherence.
2. Arbitrariness. Little or no evidence that control set (800-53) is based on evidence of what works.
3. Insufficiency. Compliance does not produce a state of security. Practitioners will tell you there are always gaps to fill.
4. Near-sighted. System focused (versus mission focused)
5. Assuming. Promotes quantitative or semi-quantitative risk assessments that take a ton of time and are usually based on guess-work.

As-Applied Problems:

6. Too difficult to do right. There is a right way, but almost nobody does it the right way.
7. Not true risk management. "Compensating controls" has a bad connotation; auditors don't want to see innovations.
    - Kristen Baldwin, Acting DASD(SE), has presented on this topic as it impacts her work as DoD's lead for systems engineering
8. Growing evidence that it is *not* getting good results.
    - See last two FISMA reports to Congress. "Federal agencies were not immune … in 2016, with over 30,899 cyber incidents that led to the compromise of information or system functionality."

NIST SP 800-171. (For more, *see* blog.trustedci.org/)

NIST SP 800-171 was created in response to Executive Order 13556 “Controlled Unclassified Information.”

What does it do?

- Standardizes how the federal government treats unclassified information that is still subject to *some* infosec requirements.
- It is a *guidance* document to help implement the executive order.
- It *does not* apply directly to non-federal entities (i.e. us), but may be incorporated into contracts, cooperative agreements, or grants.

NIST SP 800-171

Effective? . . . It depends.

1. SP 800-171 *wasn't designed* to be a comprehensive control set.
2. It is an attempt to standardize federal regulations for unclassified information. (E.g. privacy laws)
3. Mostly focused on confidentiality. We know that availability and integrity are as much or more important to this community's mission.
4. Still a compliance regime.

NIST SP 800-171

Efficient?... Seems unlikely

1. SP 800-171 is less burdensome than full-blown RMF, but in return you are getting even less security.
2. AND it is still likely to entail a lot of procedural overhead, meaning $$$$
3. Not to mention, you will still need more security on top of SP 800-171.
4. This is, however, more efficient than the unconsolidated regulations we previously had.

NIST Cybersecurity Framework (CSF)

Developed in response to Executive Order 13636, the “NIST Framework for Improving Critical Infrastructure Cybersecurity,” released in 2014. Draft version 1.1 is in progress.

More recently, Executive Order 13800 suggested using CSF for federal systems, with uncertain long-term ramifications.

Why is this important:

- Represents a partnership between the private sector and federal govt.
- Picking up steam, US led, international buy-in,
  - E.g., in August 2014, Dr. Phyllis Schneck (DHS) gave a pitch for the NIST Cybersecurity Framework at this event.
- Standardization

NIST Cybersecurity Framework (CSF)

Effective?... Hard to say.

1. Voluntary. CSF requires nothing.
   Corporate lawyers love this.
2. Broad. The control set is:
   a. Primarily pointing to other resources (includes CSC, 800-53).
   b. Not prioritized.
   c. Not as balanced toward resilience (detection, response, recovery) as first appears
3. Vague. "Tiers" are difficult to operationalize into actual measurement.
4. Similar problems with RMF relating to "risk management" and assessments.
5. Bottom line: Depends a LOT on how you use it.

NIST Cybersecurity Framework (CSF)

Efficient?... Again, hard to say.

1. Potentially efficient in that it requires nothing. Call it “highly flexible.”
2. Related resources (e.g., DHS Cyber Resilience Review) appear to have little if any relationship to the original document.
3. Have to be prepared to build an approach to using it.

Alternatives

Governance:

What does sound, sane cyber risk management entail?

Sound, sane cyber risk management

1. Roles: Senior leadership and/or asset owners are the appropriate residual risk acceptors
2. Communication: Security personnel are the SMEs who help risk acceptors make informed decisions and deal with the daily care-and-feeding.
3. Decision-making: Make tradeoffs and accept risk!
4. Policy: You may not need a lot, but you have to have a little, and you have to be rigorous across the policy lifecycle.

   Develop - Adopt - Educate - Follow - Enforce - Revise (DAEFER)

… and, skip the expensive, invalid quasi-quantitative risk assessment.

"If the highest aim of a captain were to preserve his ship, he would keep it in port forever."

- Thomas Aquinas

If you want a framework...

AFCEA's The Economics of Cybersecurity

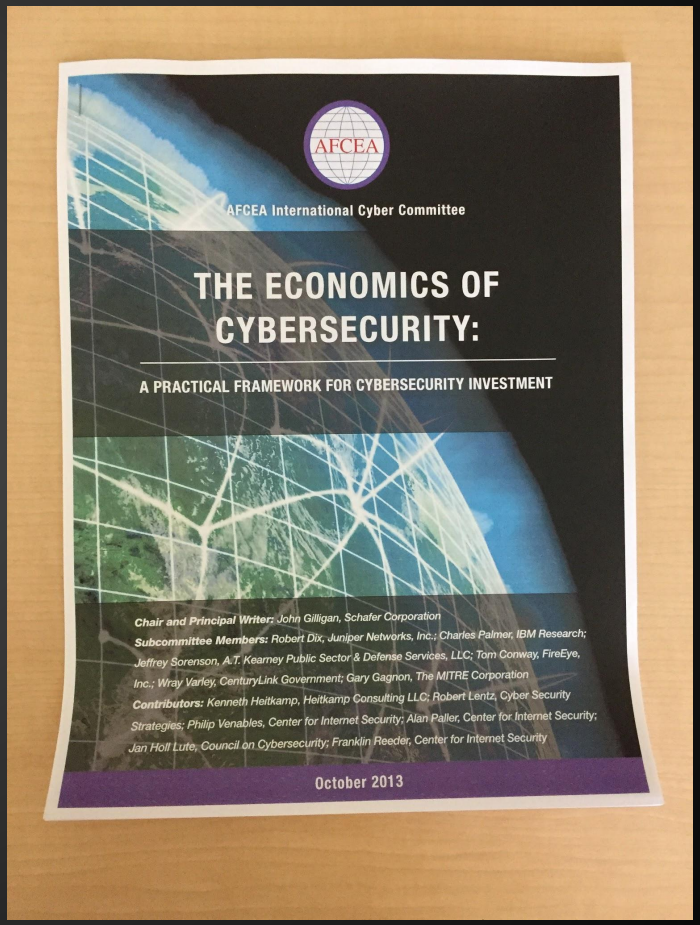
John Gilligan, fmr USAF CIO, now CIS

Background

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

Takeaways:

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



Controls:

What control sets are effective and efficient?

Center for Internet Security's Critical Security Controls (aka the Top 20)

Effective

1. Developed in a diverse, practitioner heavy environment. *E.g.*, NSA involved. (See, https://www.sans.org/critical-security-controls/history)
2. Updated frequently.
3. Testable and provable. (The plaintiffs bar and regulators will prefer this. So will technologists, engineers, and scientists.)
4. Good enough for Kamala Harris! (*See*, 2016 California Data Breach Report. The CSC's have the potential to become the de facto legal standard of "reasonable security" nationally.)

Efficient

5. Prioritized!!! (*See, esp.*, Pescatore, Back to Basics: Focus on the First Six CIS Critical Security Controls)

Australian Signals Directorate's
Essential Eight (fka Top 4)

Effective

1. Based on systematic study of actual attacks and breaches!!
2. Controls selected are those that would have prevented the most breaches

Efficient

3. There are only 8!!! (or potentially 4)
4. Prioritized by how many breaches the control would have stopped
5. Clear implementation guidance

ASD Essential 8 / CIS CSC-6.1 Cross Walk

Application Whitelisting

CSC 2.2: Inventory of authorized and unauthorized software: Application Whitelisting

Disable untrusted MS Office Macros (may be less important for science)

CSC 2.2: Inventory of authorized and unauthorized software: Application Whitelisting

Patch Applications

CSC 3.1: Secure configurations for hardware and software: Refresh/update application versions
CSC 4.5: Continuous vulnerability assessment and remediation: Deploy automated patch management
CSC 18.1: Application software security: Install latest version and all relevant patches

User Application Hardening

CSC 3.1: Secure configurations for hardware and software: Install hardened version of applications
CSC 18.4: Application software security: Test applications for common security weaknesses

Restrict Admin Privileges

CSC 5.1: Controlled use of administrative privileges: Minimize administrative privileges

Multifactor Authentication

CSC 5.6: Controlled use of administrative privileges: Use multi-factor authentication for admin acces
CSC 16.11: Account monitoring and control: Require multi-factor for access to sensitive information

Patch Operating Systems

CSC 3.1: Secure configurations for hardware and software: Refresh/undate OS versions
CSC 4.5: Continuous vulnerability assessment and remediation: Deploy automated patch management

Daily Backup of Important Data

CSC 10.1: Data recovery capability: Frequent, automatic backup for systems with sensitive data

Orange = Original Top 4; Yellow = new additions

Your Summer Reading List

AFCEA: The Economics of Cybersecurity

https://www.afcea.org/committees/cyber/documents/CyberEconfinal.pdf (8 pgs)

CIS Critical Security Controls

Poster: https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf (1 pg)

Full document: https://learn.cisecurity.org/20-controls-download (requires registration) (96 pgs)

Back to Basics

https://www.sans.org/reading-room/whitepapers/analyst/basics-focus-first-cis-critical-security-controls-37537 (5 pgs)

Australian Signals Directorate: Essential Eight

https://www.asd.gov.au/publications/protect/Essential_Eight_Explained.pdf (2 pgs)

https://www.asd.gov.au/publications/Top_4_Strategies_Explained.pdf (top 4) (42 pgs)

California Data Breach Report, 2016

https://oag.ca.gov/sites/all/files/agweb/pdfs/dbr/2016-data-breach-report.pdf (focus on the Executive Summary and Recommendations) (5 pgs)

Thank you.

Craig Jackson (scjackso@iu.edu)
Bob Cowles (bob.cowles@gmail.com)
Scott Russell (scolruss@iu.edu)

discuss@trustedci.org
cacr.iu.edu

This work was supported in part by National Science Foundation (grant 1547272).

The views and conclusions contained herein are those of the authors and should not be interpreted as necessarily representing the official policies or endorsements, either expressed or implied, of the NSF or Indiana University.