A Practical Cybersecurity Framework for Open Science Projects and Facilities

Kay Avila, Bob Cowles, Craig Jackson

2018 NSF Cybersecurity Summit
August 21, 2018

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Outline

1. Introduction
2. Cybersecurity Programs and Frameworks
3. Using the Open Science Cybersecurity Framework
    a. Mission Alignment
    b. Governance
    c. Resources
    d. Controls
4. Operations
5. Conclusion

1. Introduction

Introductions

Name, organization, why here?

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.

In our 6th year.

How is our stuff different?

1. Guidance tailored to and informed by the open science community
2. Strong attention to program fundamentals, beyond a narrow view of security controls.
3. Increased focus on *The Information Security Practice Principles** and evidence-based security practice.
4. Publicly available and free to use (unlike, *e.g.*, ISO standards)
5. Templates, templates, templates!!!

Note:

- We'll make frequent mention of resources at trustedci.org.
- We want and need to know if you are or end up using our guidance.

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

Background: Refining our Guidance

Aug 2014:

- Guide and supporting tools published to trustedci.org/guide. Developed under auspices of CTSC engagement w/ DKIST.
- Delivered first version of this training at Summit.
- Approached by NSF to draft cybersecurity section for LFM.

Jan & Feb 2015:

- Delivered first drafts of LFM section to LFO.

17 Aug 2018:

- Most recent draft of LFM section to LFO (our 6th I believe).

January 2019 (planned):

- Will publish the Open Science Cybersecurity Framework. Our best guidance and resources. More modular, but with a solid core.

Goals of this training

1. Introduce science projects, support organizations, and granting organizations to the Open Science Cybersecurity Framework, a middle path between compliance madness and complete freedom.
2. Provide actionable guidance, resources, and tools that help you get started on or get serious about your cybersecurity program .
3. Add perspective on special issues and challenges for this community.
4. Answer your questions. Hear your concerns.

Ground Rules

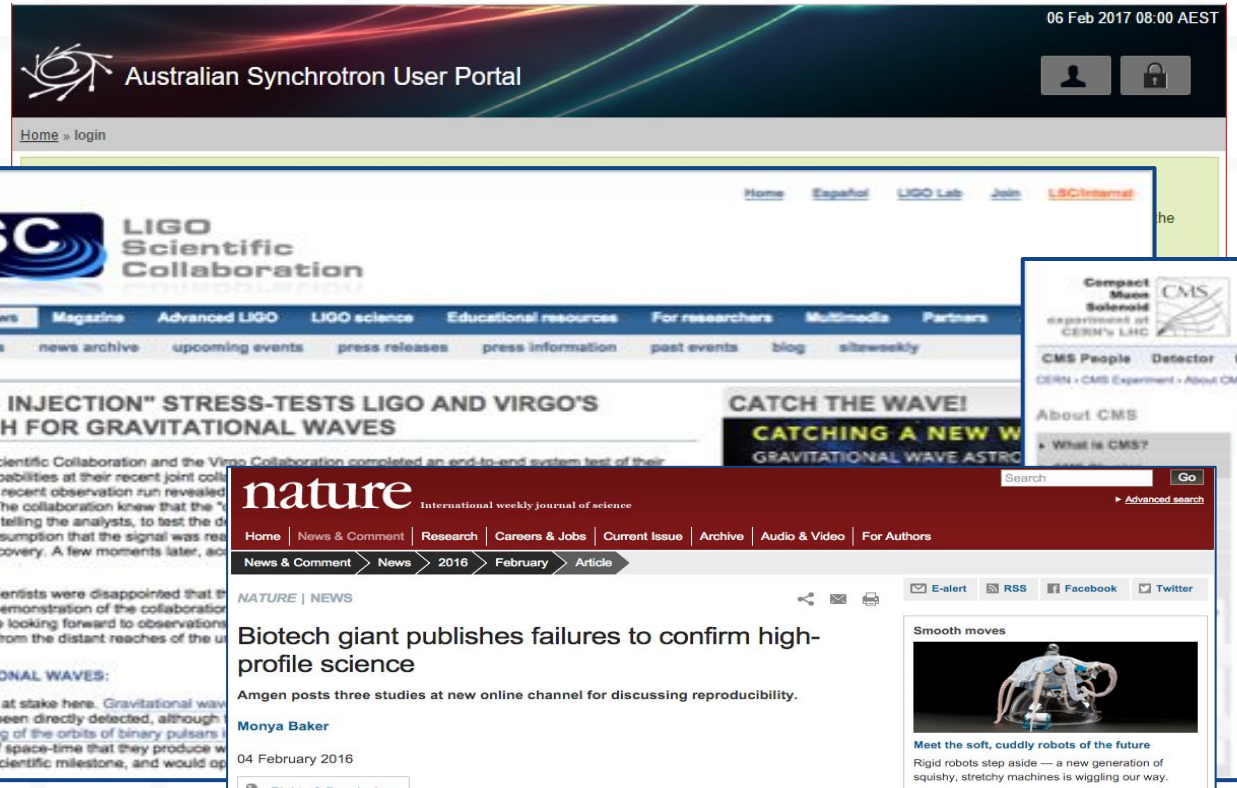
1. Interrupt us. Ask questions. Offer opinions.
   a. We will probably interrupt each other.
   b. We do have a number of designated times for Q&A.
2. Jargon alert. If we throw out a term that you don't understand, please stop us!
3. We use "information security" and "cybersecurity" more or less interchangeably.
4. Slides will be available… if not, contact us.
5. It may feel like it, but we're not going to cover everything… *e.g.*, if you're developing and distro'ing software, or have particular compliance requirements, see other training sessions this afternoon.
6. Break at about 10:30 am.
7. Please complete the training evaluation survey.
8. Please be sure you sign in.

Why Cybersecurity Matters for Open Science

Open Science and cybersecurity

- Information has always been central to science.
- Cybersecurity is about confidentiality, availability, and integrity of information and information systems.
  - Availability of instruments and systems.
  - Trust in and availability of the data.
- Reputation, trust, and other “intangibles” matter.
- Imposition of inappropriate/inefficient/ineffective compliance oriented frameworks can be a real distraction.

Science must be trustworthy & reproducible

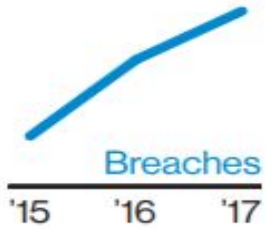


TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Verizon 2018 Data Breach Report

Education

Who	81% external, 19% internal
What	72% personal, 14% secrets, 11% medical
How	46% hacking, 41% social



Social engineering scams are targeting your employees' personal information, which is then used to commit identity fraud. Your highly sensitive research is also at risk – 20% of attacks were motivated by espionage. But sometimes the threats aren't about stealing data for financial gain – 11% of attacks have "fun" as their motive.

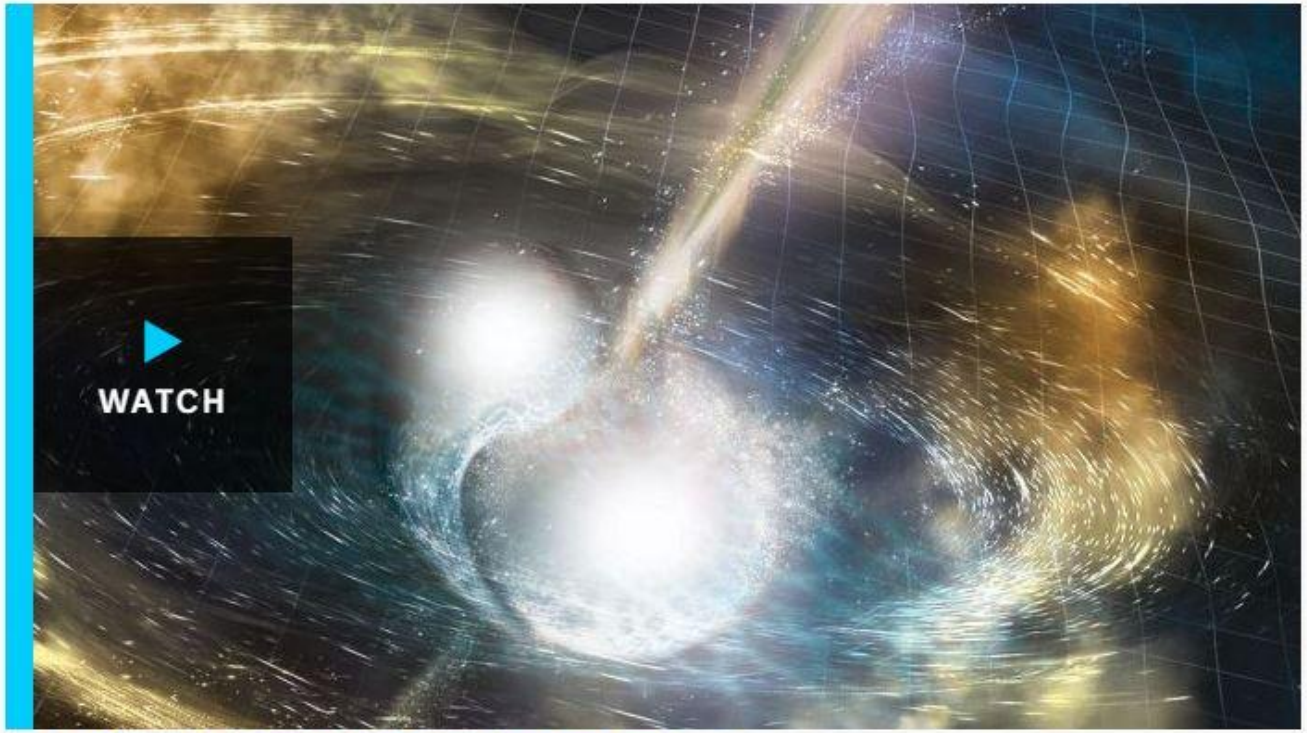
Yes, the threat is real.

"At the critical and fleeting moment, they could not move their telescope to track the gigantic explosion 130 million light years away."

Cyber attack threatened WA astrophysicists' shot at gravitational waves, colliding neutron stars

By Nicolas Perpitch

Updated 17 Oct 2017, 3:44am



VIDEO: In a galaxy 130 million lights years away two neutron stars collide (ABC News)

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

Balance is Key:
Risk versus Mission

Minimize:

Cost of breaches/incidents

+

Cost of cybersecurity program

+

Impact on science productivity

TRUSTED CI
THE NSF CYBERSECURITY CENTER OF EXCELLENCE

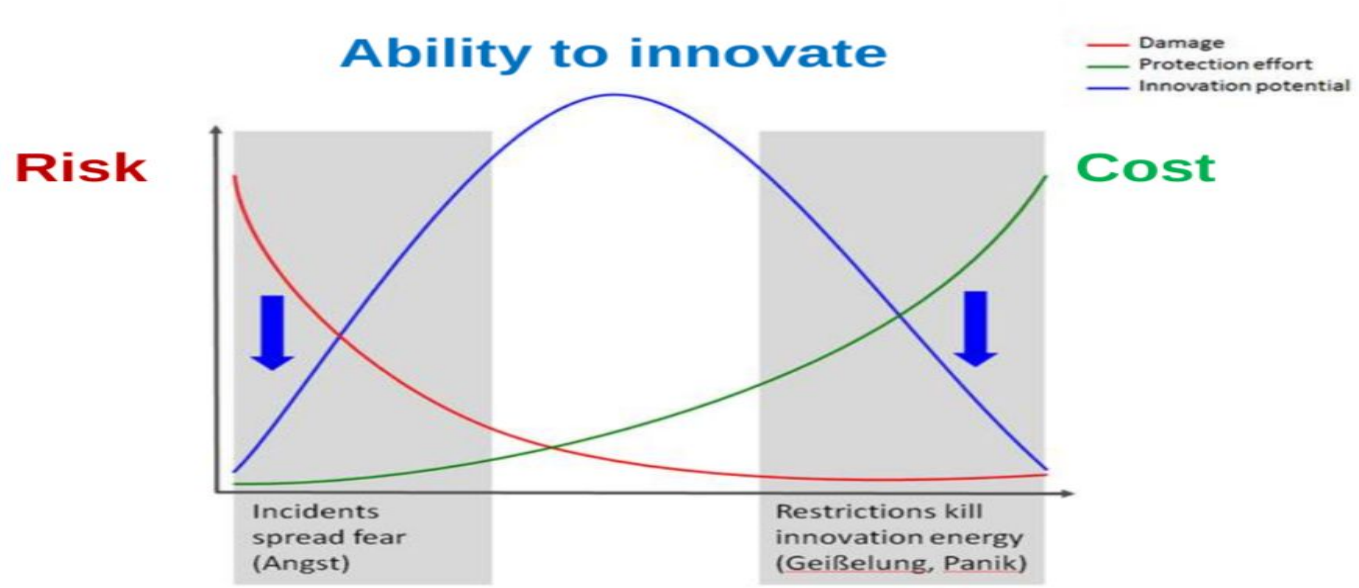
Text paraphrased from: “The Defender's Dilemma. Charting a Course Toward Cybersecurity”
http://www.rand.org/pubs/research_reports/RR1024.html

Provide guardrails, not barriers

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

SIEMENS

Too little and too strong security governance are hindering innovation



Q&A

Does anyone disagree that security is important for science?

2. Cybersecurity Programs and Frameworks

Cybersecurity Programs

What is a cybersecurity program?

An cybersecurity program is a structured approach to **develop, implement,** and **maintain** a productive organizational environment with appropriate levels of information-related risk.

A cybersecurity program addresses:

- Information classification
- Information asset inventory
- Roles
- Policies and procedures
- Program evaluation
- Risk acceptance
- Budget
- Personnel
- Controls and mitigations
- Training and awareness
- Incident response and remediation

A cybersecurity program is not

- A “plan”
- A “project”
- Simply a set of controls (aka a control set)

More than a control set? Yes!

- A cybersecurity program encompasses much more than just a control set! Selecting a control set should be part of this.
- A cybersecurity **control set** describes the controls that might be appropriate in the information environment, *e.g.*, CIS Controls, ASD Essential 8, NIST SP 800-53.
  - Controls are "administrative, technical, or physical safeguards or countermeasures operating within the environment to address a risk." (*Information Security Practice Principles*)

Cybersecurity programs are dynamic

- Program activities should evolve to address the science project or facility requirements, as
  - The organization matures
  - The threat environment changes
- Programs must adapt to
  - Key assets
  - Resources
  - Lifespan of the organization
- This dynamism should be held in shape by a structured approach (a framework)

Why approach cybersecurity as a program?

- Cybersecurity…
  - Is dynamic, complex, and multidisciplinary
  - Takes time and resources to address competently
  - Is always relevant, regardless of project phase
- Allows for…
  - Prioritization, and
  - Project management - can have multiple projects and ongoing activities in time and space to make progress.

Bottom Line

Cybersecurity programs are living breathing things

Cybersecurity Programs:
Project Phase, Size, and Complexity

Project Phase, Size, and Complexity

Phase matters: *pretty different scenarios….*

- A newly funded project that doesn't go operational for several years
- An operational facility that's been around for several years that is finally waking up to the need for a cybersecurity

Other variables:

- Overall budget and IT budget
- Cybersecurity budget?
- # of personnel
- Geographic and institutional distribution
- Role and importance of information assets
- Institutional support

Project Phase, Size, and Complexity

Our working assumptions:

- You have some freedom or need to define a program for your project and facility. No one is going to do it all for you.
- You are not so resource constrained that some cybersecurity basics are impossible.

Cybersecurity Programs:
Kickstarting a Cybersecurity Program
A few case examples

Case 1… a newly funded facility, under construction

Architect, select, and build information assets and environments that are more secure and resilient from the start!

Start early and bake it in at the beginning

Case 2… an operational facility

1. Identify Critical Risks
   Grey pigeons. High frequency incidents. Reduce frequency and aggregate impact.
   Black swans. Reduce impact / contingency planning.
2. Identify the “Crown Jewels”
3. Identify Governance and Control Gaps
   a. Roles and responsibilities. Who has the ball?
   b. Think CIS Controls’ top 5 or 6, aka “cyber hygiene.”
4. Implement Targeted Controls
   a. *Low-hanging fruit first* (low cost, high positive impact)
   b. Sequence! Can’t and probably shouldn’t do everything at once.

Case 3... a newly funded project housed in one or two academic institutions

Your first step may be to talk to your department, research computing center, or security office.

Must Do's:

1. Determine what you have (parallel / iterative)
   - Inventory Assets
   - Identify Stakeholders
   - Categorize Data
   - Determine Project Information Flows
2. Determine what the institution provides
3. Determine who is responsible for controls
4. Fill Gaps
5. Ensure operational activities are covered

Caveat: Institutional priorities are likely different from project priorities

Webinar

https://www.youtube.com/watch?v=ki1ppha6U6o

Slides

https://scholarworks.iu.edu/dspace/handle/2022/21260

Q&A

Who here is at the “building” stage?
Who’s at the “improving” stage?

Cybersecurity Frameworks

Why adopt a cybersecurity framework?

- Provides structure and a common language
- Increases non-expert (management, auditor, program officer) confidence that the cybersecurity program is well-grounded
- NOTE: Selecting a framework is different from selecting a baseline control set.
- Most recent cybersecurity frameworks are at least nominally about risk management, which can be a good thing.

Risk!

Why Risk Management? *Flexibility*

- Compliance or rule-based approaches are generally inappropriate for infosec.
  - *Dynamic hazard, relatively new, relatively low risk (for now)*
  - *Security is not a solved problem*
  - *Compliance is good when a solution has been proven to work.*
- Allows for mitigation, transfer, avoidance, and acceptance of risk.
- Well-suited for organizations with limited resources and time. (Risk acceptance is still on the table.)

Some Risk-Oriented Frameworks

- NIST Risk Management Framework (RMF)*, **
- NIST Cybersecurity Framework (CSF) **
- HIPAA Security Rule*
- ISO 27005
- COBIT
- OCTAVE
- Open Science Cybersecurity Framework

** blended or corrupted into compliance regimes*

*** discussed shortly*

What do you choose?
Remember, balance is key….

Effective: Inclusive. Evidence-based. Adaptable.

Efficient: Doable. Affordable. Prioritized. Time-saving.

Special Topic

NIST's Frameworks

Are NIST's framework a good fit for open science?

Probably not. We're going to explain why. Other trainings can help you figure out how to survive them.

We're going to talk about two NIST frameworks:

- NIST Risk Management Framework (ala FISMA)
- NIST Cybersecurity Framework

Why avoid existing NIST frameworks?

Processes found in the existing frameworks (NIST RMF; NIST CSF) make questionable assumptions:

1. Assume cybersecurity presents a measurable environment with some historical stability (e.g., actuarial history).
2. Assume organizations have the time, money, and expertise to execute intensive procedural / documentation regimes.

Why avoid existing NIST frameworks?

As a result:

1. Much time and money has been wasted on quasi-quantitative risk assessments with little or no validity… rather than getting the basic processes and protections in place.
2. Frameworks like NIST RMF give lip service to risk management, but have devolved into massive documentation games and checklist maintenance.

NIST Risk Management Framework (RMF)

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

We have seen talks and presentations at past Summits making the case that NIST RMF and NIST SP 800-53 (big ol' control set) are obvious sources of procedural and control selection guidance.

Yet, people in the trenches have also told harrowing stories of RMF in application. And, there are clearly other options (incl. other NIST products).

*Updated to Federal Information Security Modernization Act of 2014 (FISMA 2014)

NIST Risk Management Framework (RMF)

Efficient? … Heck no!

1. Assumes you have a lot of time, money, and expertise to devote to cybersecurity compliance.
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

Effective? … It's costly but does it get us security?

Prima Facie 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 guesswork.

NIST Risk Management Framework

Effective? … It's costly but does it get us security?

As-Applied Problems:

1. Too difficult to do right. There is a right way, but almost nobody does it the right way.
2. 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
3. Growing evidence that it is *not* getting good results.

   See recent FISMA reports to Congress. "… agencies endured 35,277 cybersecurity incidents in Fiscal Year (FY) 2017, which is a 14% increase over the 30,899 incidents that agencies reported in FY 2016, with five of the FY 2017 incidents reaching the threshold of "major incident" due to their impact"

The conclusion reached by this analysis is that, despite the comprehensive nature of the NIST Risk Management Framework and its unassailable underlying logic, it has not proved practical for organizations who are struggling to determine where to invest in cyber security and, in particular, how much investment in cyber security is warranted.

-- *AFCEA's The Economics of Cybersecurity*

Rev. 2 draft of the NIST RMF weighed in at a hefty 149 pages, up from 102 pages from Rev 1 in 2010. Post incident data almost invariably points out IT and security operational failures as the enabling factor, not lack of heft in risk management documents and policies. The good news is NIST has produced some RMF quick start guides. The bad news is the "Implement" phase has no quick start guide, which is kind of a symptom of the overall problem.

-- John Pescatore, commenting on draft RMF 2.0, SANS NewsBites Vol. 20, Num. 064, 14 August 2018

NIST Cybersecurity Framework (CSF)

Developed in response to Executive Order 13636, the “NIST Framework for Improving Critical Infrastructure Cybersecurity,” released in 2014. Version 1.1 was released April, 2018.

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
- Standardization

NIST Cybersecurity Framework

Effective? … Hard to say

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

NIST Cybersecurity Framework

Efficient? … Again, hard to say

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

New Approach at NIST?

NIST's willingness to say aloud that the old guidance [concerning passwords] was not correct is emblematic of a new approach we have been seeing at NIST. An equally impressive example of the shift to evidence-based guidance is their semi-public suggestions that the Australian "Essential Eight" or the Critical Security Controls "Top 5" (the two are nearly identical) are acceptable approaches to prioritizing actions that should be taken first in implementing the NIST Security Framework. Both the Essential Eight and the Top 5 are based on empirical evidence of what mitigations block and help mitigate damage from known attacks.*

* Alan Paller, SANS NewsBites,Vol XIX #62 August 8, 2017

Q&A

What does a sound, sane cybersecurity risk management framework entail?

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

Sound, sane risk management framework

Comprehensivity - Cover mission requirements

Opportunity - Take advantage of host institution environment

Rigor - Implement evidence-based controls

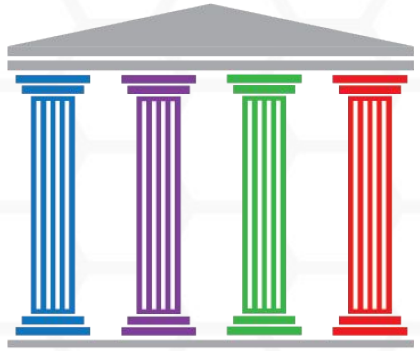
Minimization - Limit and eliminate unnecessary complexity

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

Open Science Cybersecurity Framework
The Pillars



Mission Alignment

Information classification, asset inventory, external requirements

Governance

Roles and responsibilities, policies, risk acceptance, program evaluation

Resources

People, budgets, services and tools, lifecycle

Controls

Procedural, technical, administrative safeguards and countermeasures

3. Using the Framework

Section 3: Using the Framework
Outline

3.a Mission Alignment

3.b. Governance

3.c. Resources

3.d. Controls

3.a. Mission Alignment

What is “Mission Alignment?”

1) The cybersecurity program is focused on enabling the organization’s mission and protecting its interests (e.g., the science mission, reputation, safety of personnel, staying on the right side of the law and ethics).

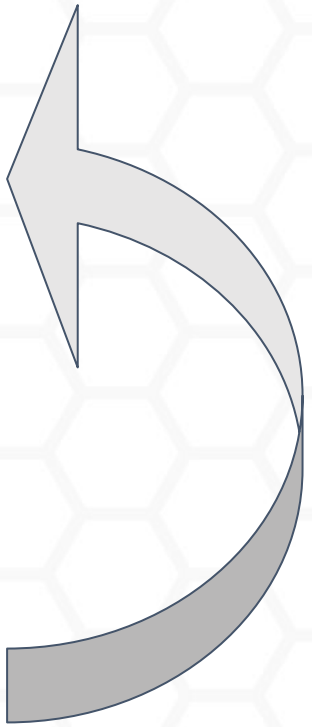
2) Cybersecurity risk management decisions are made with organization’s mission in mind.

"CIA" and Controls in Perspective

Project Mission & Interests
Trust in scientific results, reputation, safety

'CIA' Security Objectives
Confidentiality, Integrity, Availability

Controls
E.g. 2FA,network monitoring



By focusing on preventing "losses of information security," CIA objectives sit between the fundamental reasons why we protect info assets and the controls we put in place.

CIA Triad of Security Objectives

Confidentiality Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information. A loss of confidentiality is the unauthorized disclosure of information.

Integrity Guarding against improper information modification or destruction, and includes ensuring information authenticity. A loss of integrity includes the unauthorized modification or destruction of information, and the unauthorized control of an information system.

Availability Ensuring timely and reliable access to and use of assets. A loss of availability is the disruption of access to or use of an asset.

Mission Alignment:
Information Classification

Information Classification

Information has varying degrees of organizational value, sensitivity, and protection requirements.

- Key factors to consider in analyzing the anticipated impact of security incidents.

In most cases, 3 or 4 categories are sufficient:

- *i.e.* public, internal, controlled

Information Classification

Develop policy specifying core procedures regarding treatment of different categories of information:

- creation, processing, transmission, storage, and disposal.

Information asset protection requirements are then determined by the protection requirements of the category of information.

Mission Alignment:
Information Asset Inventory

Information Asset Inventory

Organizational identification and location of information assets is a prerequisite to competently securing those assets.

Producing and maintaining an inventory of information assets is a basic process in establishing a mission-aligned program.

Information Asset Inventory

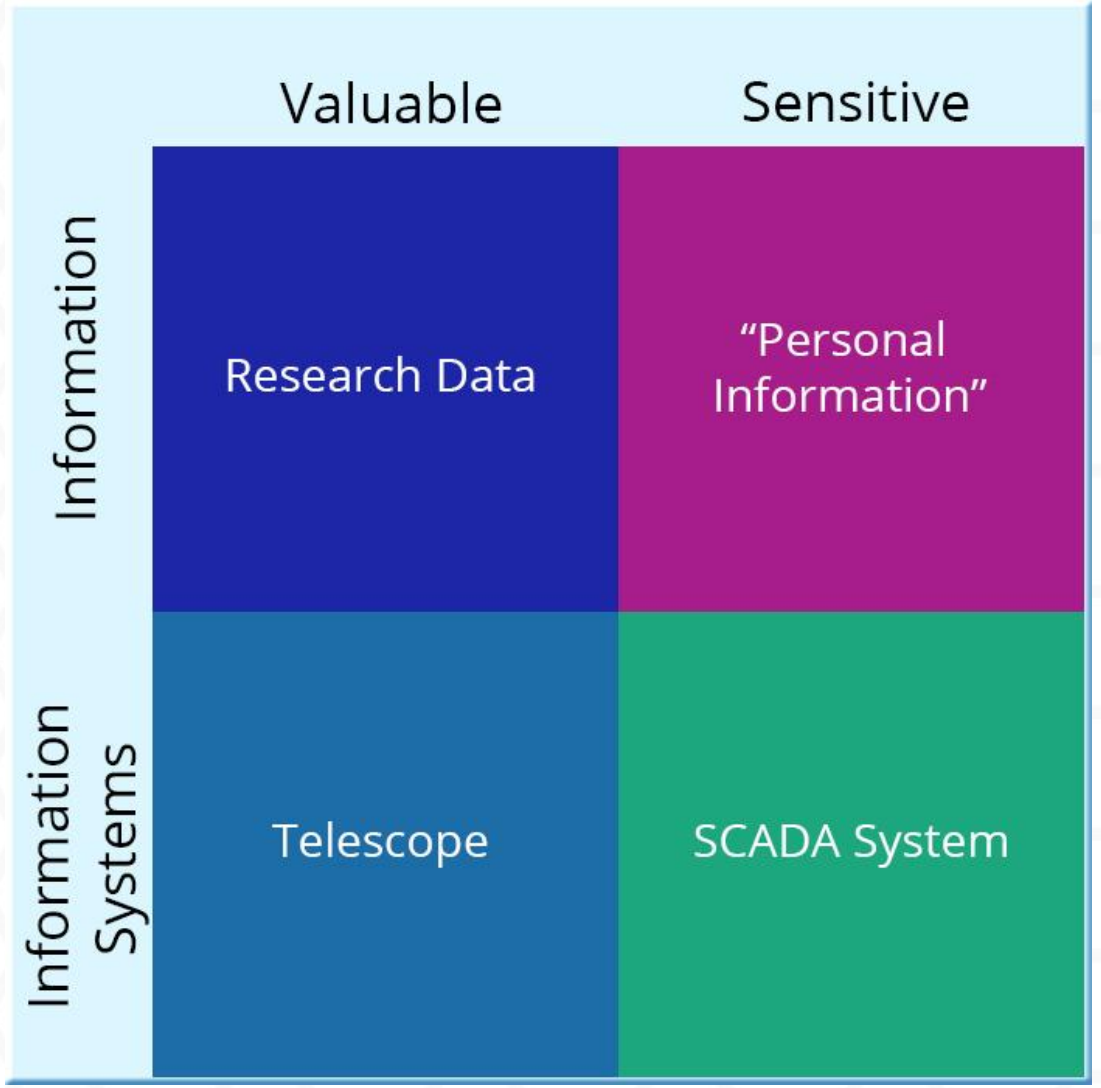
The asset inventory can be built

- With the assistance of automated asset discovery tools but manual additions will certainly be required, or
- Manually using publicly or commercially available templates or worksheets or by constructing a custom database.

Information Assets

The Open Science Cyber Risk Profile (OSCRP) guides determination of critical assets and classifying them appropriately

https://trustedci.org/oscrp/



Tips for identifying information assets

- Create and maintain solid documentation of what is actually there.
- Start with your *information* inventory (*vs.* information systems) and capture data flows.
- Think in terms of types of information and information systems; get more detailed as needed.

Information Asset Inventory

Take the opportunity to get a handle on the security objectives for those assets.

The inventory might include a number of details, but at a minimum:

- Identify the asset and
- Indicate the classification of the information or system.

See https://trustedci.org/guide for templates

Information Data Details

- What's included in this data?
- Why do we have it? Where is it coming from, and what do we use it for?
- How is this dataset stored?
  - Format
  - Location
  - Backups
- Where should this data travel?
  - Who and what systems should be able to access?
  - How will it get there?
  - How is that movement protected? (e.g., authentication, encryption)
- What, if anything, sets this data apart from other things in the type?

Information System Details

- Hardware specs & serial numbers (if applicable)
- Software packages & major version numbers
- What data does this system touch?
- How does that data get in and out, and where does it go to/come from?
- What can this system control? How is that done?
- What does normal operation of this system look like? What runs on this system?
- How do we know when it's not behaving?
- What administrative systems control and document this system?

Q&A

Success stories
Identifying your assets and maintaining that up-to-date picture??

Any tricks or templates or deliverables you'd be willing to share?

Mission Alignment: **External Requirements**

External Requirements

Historically, open science has a lot of freedom. *E.g.*, The NSF Large Facility cooperative agreements give a LOT of breathing room.

Other potential sources of external requirements are non-trivial:

- Statutes, regulations, and case law (*e.g.*, state or federal privacy laws)
- Contractual terms
- Institutional or parent organization policies
- Large Facility Manual
- Miscellaneous officious bureaucrats (j/k)

Remember, you have some choice and/or ability to negotiate *some* of these requirements.

External Requirements

Big takeaways:

1) There's no excuse for being ignorant of existing external requirements.
2) Some continued vigilance is required to make sure you are in line with law and applicable policy.
3) Unless you are a lawyer *and* a lawyer for the awardee, don't act like one. Get help; transfer the risk.

Mission Alignment:
External Requirements
NSF Cooperative Agreements

NSF Cooperative Agreements

Information Security Requirement

- Incorporated in NSF's Supplemental Financial and Administrative Terms and Conditions*
- Purpose is to help ensure that NSF Large Facilities and FFRDCs have **policies, procedures, and practices to protect research and education activities** in support of the award
- Terms or requirements like this are increasingly common at the proposal stage.
    - * https://www.nsf.gov/awards/managing/co-op_conditions.jsp

In Supplement to CA-FATC LF and CA-FATC FFRDC:

"Security for all information technology (IT) systems employed in the performance of this award, including equipment and information, is the awardee's responsibility.

"Within a time mutually agreed upon by the awardee and the cognizant NSF Program Officer, the awardee shall provide a written Summary of the policies, procedures, and practices employed by the awardee as part of the awardee's IT security program, in place or planned, to protect research and education activities in support of the award."

In Supplement to CA-FATC LF and CA-FATC FFRDC:

"The Summary shall describe the information security program appropriate for the project including, but not limited to: roles and responsibilities, risk assessment, technical safeguards, administrative safeguards, physical safeguards, policies and procedures, awareness and training and notification procedures in the event of a cyber-security breach. The Summary shall include the awardee's evaluation criteria that will measure the successful implementation of the IT Security Program. In addition, the Summary shall address appropriate security measures required of all subrecipients, researchers and others who will have access to the systems employed in support of this award."

In Supplement to CA-FATC LF and CA-FATC FFRDC:

"The Summary will be the basis of a dialogue which NSF will have with the awardee, directly or through community meetings. Discussions will address a number of topics, such as, but not limited to, evolving security concerns and concomitant cyber-security policy and procedures within the government and at awardees' institutions, available education and training activities in cyber-security, and coordination activities among NSF awardees."

Mission Alignment:
External Requirements
NSF Large Facilities Manual

NSF Large Facilities Manual

Section 5.3 states in part: “This section, to be written, will describe what NSF considers to be a fundamental set of IT security requirements that facilities should consider in developing and deploying their IT plans, policies and procedures. These minimal requirements and their associated evaluation criteria, as provided by the facility and agreed to by NSF, are used as part of NSF’s facility oversight and review process.”

NSF Large Facilities Manual

- Since 2014, Trusted CI has worked with the Large Facilities Office to create and refine a draft. Over the last year, we have vetted that work with the Large Facility Security Team. https://trustedci.org/lfst/
- Last draft and comments sent on August 17, 2018. Disposition of content in NSF's hands is TBD.
- Anticipate draft for public comment on Federal Register in mid-October 2018.
- Final publication of the new Manual that includes the cybersecurity material is expected in the late Summer 2019.

“Musts” from our Spring 2018 draft.

1. Large Facilities must establish and maintain an information security program and provide a written Summary of that program to the cognizant NSF Program Officer.
2. Large Facilities must develop an information classification policy that specifies core procedures regarding the creation, processing, transmission, storage, and disposal of the different classes of information.
3. Large Facilities must identify the information assets associated with mission critical or processes or information flows and with the processing or storage of sensitive data.
4. Large Facilities must identify external requirements that impact the information security program.
5. Large Facilities must establish, educate on, and enforce core policies on information security-relevant roles and responsibilities for all classes of personnel, including staff, facility leadership, affiliates, and external users.
6. Large Facilities must establish an explicit role responsible for the facility’s information security program.
7. Large Facilities must identify the information security policies necessary to govern information security practices, and implement processes to develop, adopt, educate personnel on, enforce, and as necessary revise those policies.
8. Large Facilities must apply information security policy to all entities who will have access to the assets employed in support of the award, including subrecipients, researchers, and cloud service providers.
9. Large Facilities must develop or adopt and implement a process for internal communication about information security risk that supports risk mitigation, avoidance, transfer, or acceptance decisions by facility leadership or asset owners.
10. Large Facilities must plan for and facilitate evaluation of their information security programs.
11. Large Facilities must provide adequate resources for a competent information security program to facilitate the range of activities described over the project life cycle.
12. Large Facilities must budget for information security.
13. Large Facilities must allocate personnel effort to information security.
14. Large Facilities must consider information security when selecting and adapting to the use of third party services.
15. Large Facilities must adopt and utilize a baseline control set or sets.
16. Large Facilities must address whether specialized or alternative information security controls are warranted to support the science mission.

3.b. Governance

Governance: Outline

- Relationships
- Project Management
- Roles and Responsibilities
- Risk Acceptance
- Policy Development
- Policies that address NSF's External Requirements
- Program Evaluation

Defining “Governance”

“The manner in which something is governed or regulated; method of management, system of regulation.”

-- OED online

How will your cybersecurity program be governed?

Governance
First steps

1. Determine whether and how relationships and existing policies and process will help or burden you.

2. Develop core cybersecurity policy with special attention to roles and responsibilities, and risk acceptance.

Governance:
Relationships

Governance: Relationships …

… play a key role in a cybersecurity program

Cyberinfrastructure (CI): Research environments that support advanced data acquisition, data storage, data management, data integration, data mining, data visualization and other computing and information processing services distributed over the Internet beyond the scope of a single institution.*

*https://en.wikipedia.org/wiki/Cyberinfrastructure

Project Relationships

You are not alone

CI Projects are increasingly distributed, international, multi-institutional, and interdisciplinary, but highly interconnected. Virtual project teams are commonplace.

While this can create challenges, it also creates opportunity.

Challenges

Complexity

- Disparate policies and requirements among collaborators - establishing MOUs
- Cultural differences (open research environments vs. restrictive govt labs); information sharing, communications, different compliance reqs
- Larger attack surfaces: users, servers, network connections, inconsistency with administration and management
- Specials: ICS/SCADA, one of a kind research data
- More actors: hacktivists, governments, bad users

Opportunity

"I've got your back"

- Collective knowledge of a distributed team can be a resource of support. "Has anyone seen this unusual network traffic?"
- Sharing event information allows improved detection ability and response times. "Mass scanning from IP address 201.234.178.62, suggest blocking"
- Ad-hoc support in times of need.
- Third-party services for $$ when you really need help

DIY

HELP!

Governance:
Project Management

Project Management*

- Plans, goals, objectives, milestones, timelines, deliverables…. Your friends!
- Enables prioritization. (A novel idea for many infosec people.)
- Critical to turning seemingly intractable problems into workable issues.

* Shout out to Gemini Observatory and UNH Research Computing Center for sharing with us how project management enables security.

Governance:
Roles and Responsibilities

Key Roles

Senior Management (e.g., PI, Director, CIO)

Takes active role in allocating adequate resources, addresses program governance, accepts residual risk, and follows information security policies

Asset "Owner"

Has control over the information or technology; understands risks to the asset and ensures appropriate controls are in place while the asset is being developed, produced, maintained, and used

Chief Information Security Officer (CISO)

Knowledgeable in information security, understands how information assets relate to the organization's mission, effectively communicates the issues and the tradeoffs; empowered as a decision-maker and key stakeholder where expert and timely action are required to protect organizational interests

Key Cybersecurity Responsibilities

Leadership has responsibility for ensuring the project has an effective cybersecurity program.

- Promote the importance of the program
- Delegate security responsibilities
- Play an active role in risk management decisions, including risk acceptance.
- Lead by example

Governance:
Risk Acceptance

Risk Definitions

- Residual risk is the risk left after controls are applied. In cybersecurity (as in most of life), it is never zero.

- Risk acceptance is the heart and soul of risk management, whether the risk is accepted without mitigating controls or is residual risk.

Risk Acceptance

- Typically done when the cost of mitigating the risk exceeds the expected benefit
- Needs to be explicitly performed by decision makers after being informed of residual risk and options for reduction
- Must be reviewed periodically as parameters change
- Does not reduce the actual risk

Risk Acceptance Responsibilities

Risk Acceptor: Weighs risks against project mission and accepts residual risk. Must have broad view of project, have ability to control the information assets, and is responsible for the outcome of accepting those risks, *e.g.*, Management, PI, technical lead.

Cybersecurity Lead: Responsible for cybersecurity implementation & gauging residual risk. Must translate technical issues into management language, helping risk acceptors make informed decisions, *e.g.*, IT Security Professional, senior technical person.

AFCEA's The Economics of Cybersecurity

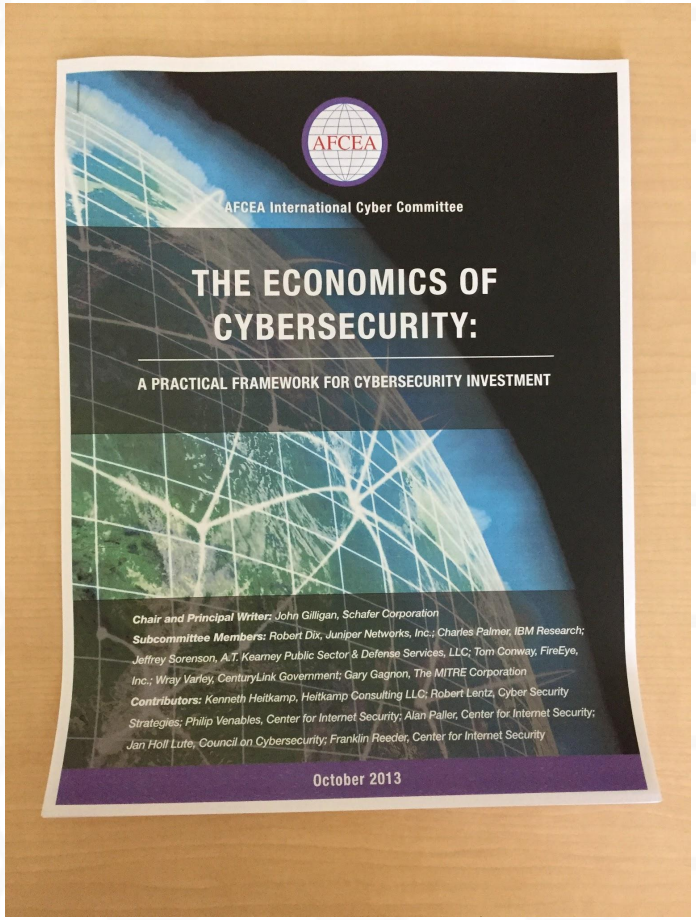
John Gilligan, fmr USAF CIO

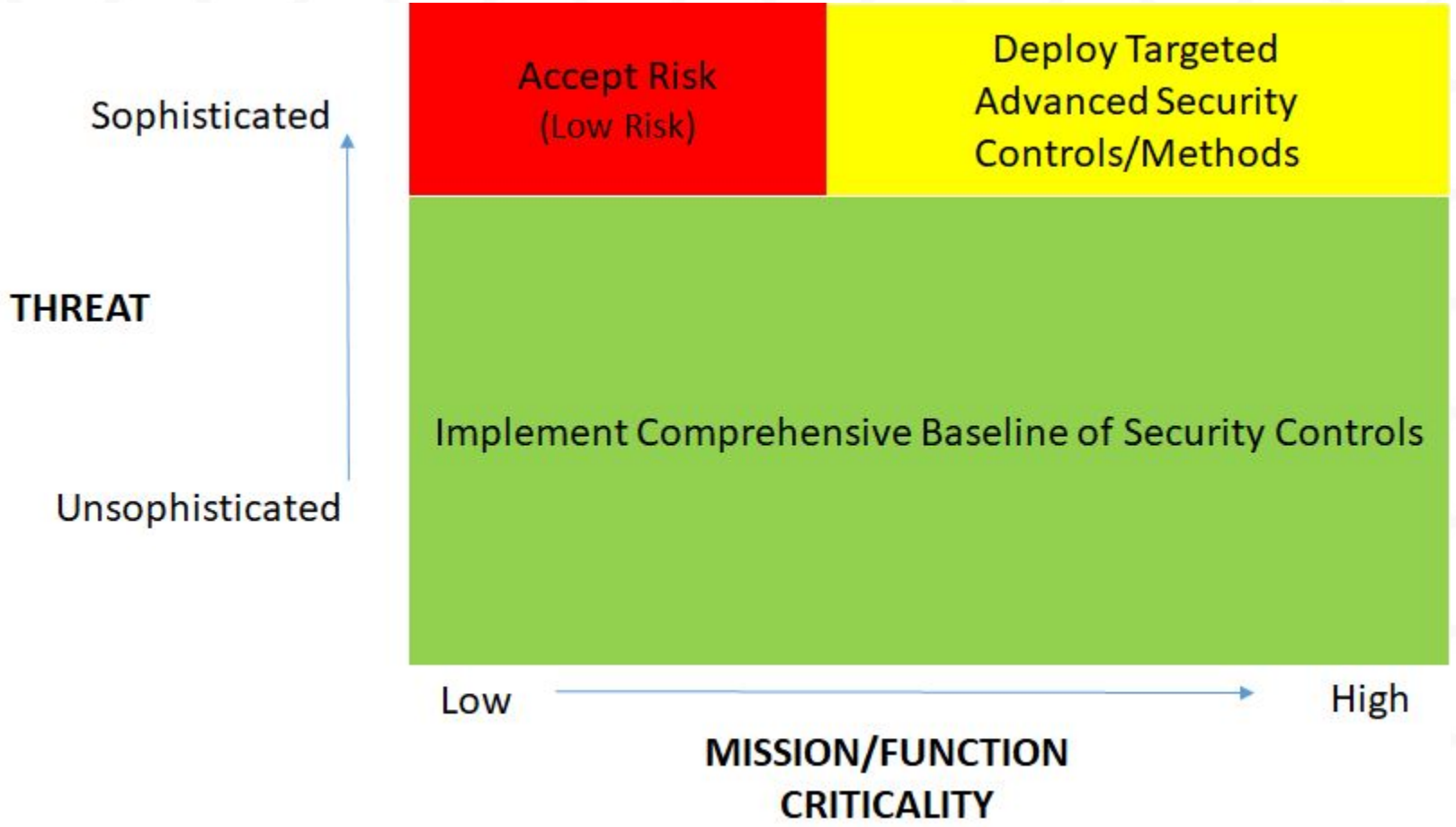
Background

- 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

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

- Thomas Aquinas

Governance:
Policy Development

How much policy is enough?
How much policy is known to cause cancer in lab rats?

Policy Development

You may not need a ton of written policy, but you need some.

Results in:

- Reproducible, communicable, and enforceable policy and processes
- Artifacts that can be critiqued and evolved
- Include instructions for requesting policy exemptions

The Policy Lifecycle ©

(DAEFER?... Without "adopt" its just DEFER.)

1. *Develop*
2. *Adopt*
3. *Educate*
4. *Follow*
5. *Enforce*
6. *Revise*

The policy valley of death

Policy Development: Tips and Gotchas

Please do:

a. Involve stakeholders (yes, even the relevant lawyers)
b. Prioritize
c. Use templates, examples
d. Ask for help
e. Share the resulting policies and train your personnel

Please don't:

f. Fall into the policy valley of death
    i. Allow policies to be developed and filed away without a formal approval process
    ii. Assume people will read them without training/education
    iii. Develop policies no one can or will enforce
g. Work in a vacuum
h. Assume you need one of each
i. Be afraid to take this seriously
j. Underestimate the power of v2

Templates!

We will refer to templates found at:

https://trustedci.org/guide

Cautionary Note: You will *have to* make these your own.

Policies We'll Highlight

- Master Information Security Policy and Procedures (MISPP)
- Incident Response Policies & Procedures
- Access Control Policy
- Acceptable Use Policy (AUP)
- *A note about Privacy Policies*

(But… physical security, disaster recovery, asset management, HR-specific, "specials" specific…. other policies can be critically important for your project.)

Master Information Security Policy and Procedures (MISPP)

Purpose: Core, general policies + guide for navigating the full corpus of policies and procedures.

Audience: You and all your stakeholders.

- Roles & Responsibilities (… CISO, Leadership)
- Developing, Implementing, and Maintaining Our Cybersecurity Program (… core processes)
- Resources & Key Contacts (… we're here to help)
- Other Policy and Procedure Documents (… a gateway of sorts)
- Enforcement provisions
- Terms & Acronyms
- *… plus anything else so central to the program that it warrants stating here*

Incident Response Policy

Purpose: Decide and document what to do in the event of a security incident BEFORE one happens, so that the response can be both rapid and well thought out.

Audience: IT and helpdesk staff, incident response team

- Define priorities for IR (e.g., relative importance of gathering forensic data vs. minimizing downtime)
- Who need to be notified, when, how, by whom; contact info
- Define who is responsible for which decisions
- Lay out response procedures for grey pigeon and black swan events
- IR team communication guidelines
- Specify when and how response procedures will be tested

Access Control Policy

Purpose: Define how access to various information assets (both systems and data) will be mediated, as well as who will be allowed access to what.

Audience: All users, stakeholders, and IT staff.

- You must first know what your assets are and need a data classification schema
- Least privilege principle
- Authentication vs. authorization
- Impacts every control

Acceptable Use Policy (AUP)

Purpose: Establish a code-of-conduct for all users on the usage of a resource/information system.

Audience: You and all your stakeholders.

- Establishes authority and defines rights and responsibilities of all users
- Consequences of infractions to policy (suspension, legal, criminal)
- Reduce Liability: disclaimers, no warranties
- Other Policy and Procedure Documents (Privacy, Password, management, Academic citation)
- Contact Information (General support, Emergency/Security)

Positive Statement	1. Purpose of [this system, organization, whatever]
General Good Behavior	2. Your use must be in alignment with [the purpose]
Specific Good Behavior	3. You must [responsibilities] a. Make a strong password
Specific Bad Behavior	4. You must not do things contrary to [the purpose], including, but not limited to… a. Mining bitcoin b. … [nice to explain why, but don't have to]
Negative Consequences	5. Or else, you will be [nuked from orbit, scolded, cut off]

A note about privacy policies …

We didn't template one, on purpose.

- You may or may not be required to have one
- You may or may not want to have one
- Getting input is key…. think general legal counsel
- International collaborations complicate things in a hurry

Want a template? Check out the BBBs

Governance: Bonus Hint
Policies that Address the NSF External Requirements

“Roles and Responsibilities”

Trusted CI Resources:

- *Master Information Security Policy and Procedures (MISPP)*
- *Acceptable Use Policy (AUP)*

“Risk Assessment”

Trusted CI Resources:

- *Information Asset Inventory*
- *Risk Assessment Table (if you can’t help yourself)*
- *Open Science Cyber Risk Profile (OSCRP)*

"Technical, Administrative, Physical Safeguards"

Trusted CI Resources:

- *Access Control Policy*
- *Asset-Specific Access and Privilege Specification*
- *Password Policy*
- *Physical Security Policy*
- *Disaster Recovery Policy*
- *Incident Response Policy and Procedures*

"Awareness and Training"

Trusted CI Resources:

- *Information Security Training and Awareness Policy*
- *Trusted CI "Cyber Hygiene" Information Security Training Slide Deck*

"Notification Procedures"

Trusted CI Resources:

- *Incident Response Policy and Procedures*

"Evaluation Criteria"

Trusted CI Resources:

- *Master Information Security Policy and Procedures (MISPP)*

"Appropriate Security Measures for all"

Trusted CI Resources:

- *Acceptable Use Policy (AUP)*

Governance:
Program Evaluation

What are we evaluating?

Measuring cyber wellness

Health	How functional are we? How sick?
Maturity	Do we have the right policies, procedures, processes, and resources in place?
Susceptibility	Can we keep malicious actors at bay?
Resilience	Will we bounce back when things go wrong?
Compliance	Are we doing everything someone else told us to do?
Growth	Did we make improvements over time?

Program Evaluation

- Periodically evaluate the effectiveness of existing controls
- Identify and address new risks as environments change.
- There exist a variety of tools and methods for evaluating information security programs:
  - Some focus on process maturity
  - Others gauge the effectiveness of controls and the organization's cybersecurity "hygiene" or "health."
- These tools utilize a variety of metrics and may also assist organizations in developing long term goals for their information security programs.

Opportunity: External Reviews

- External peer or expert reviews can provide added objectivity, as well as fresh perspectives.
  - "Blue team": Can be friendly / trusting (e.g. Trusted CI engagements)
  - "Red team": Depth, Adversarial (e.g., pen-testing)
- Reviews can provide invaluable perspectives on:
  - Maturity of one's program
  - Possible areas of improvement
  - New strategies
- Specify the focus/standard used for the review
- Specify the review deliverables and audience(s)

Opportunity: Perform Self Assessments

- Provide the organization, particularly senior management, with a report on how cybersecurity resources are currently deployed and the gaps to be prioritized for future efforts.
- Invaluable for establishing trust between senior management and the cybersecurity team
- Lower cost than an external review:
  - Security Program Assessment Tool in the EDUCAUSE Library
  - Cyber Security Evaluation Tool (CSET) from Department of Homeland Security

Opportunity: Perform Self Assessments

- Blue-ish:
  - Project based: Did we meet the objectives in our plan?
  - Standards based: How do we compare to the archetype?
  - Benchmark based: How do we compare to our peers?
- Red-ish:
  - Table top exercises
  - Simulated incidents
  - Real incidents: How did we do during a real incident? What can we improve?

Opportunity: Evaluate Incident Response

- Incident detection, response, and recovery test the program's administrative, technical, and physical controls
- Incident *post mortems* can:
  - Identify significant program gaps,
  - Clarify processes, and
  - Generate input for refining controls
- Table-top exercises test the incident response plan in advance of an actual incident.
- Red team exercises and penetration tests can provide even more realism

The Positives Matter

- Security is about surviving ***and*** thriving.
- Celebrate both.

3.c. Resources

Resources
First steps

1. Develop a budget
    a. Decide what is in/out of the budget (staff, tools, training)
    b. What are good IT practices vs. cybersecurity?
2. Invest in people
    a. A variety of specific skills are required
        i. Technical and person skills
        ii. Understanding how things go wrong
    b. Need frequent training and contact with peers (more about this later)

Budget

- Security costs money.
  - Hint: Joining forces and sharing practices and information leads to economy of scale.
- Cybersecurity budgets lie between 3% to 12% of IT budgets. (Smaller budgets have higher percentages)*
- Variance on what is included in cybersecurity budget
- Distinguish between good practices (business and IT) and actual cost of cybersecurity

* See: 2016 NSF Cybersecurity Summit Report for details: http://hdl.handle.net/2022/21161, pg. 101

People

Invest in people!

- Hire *security practitioners*, and support their professional development. Consider: Training (more later),
- Collaborate across silos.
- Build partnerships, leverage collective action, look to similar entities doing things well.

People: Required Skills

- *Technical* skills around networks, operating systems and applications, security tools
- *Teaching* skills to educate users on cybersecurity
- *Communication* skills to put cybersecurity risks into terms relating to the scientific mission
- *Negotiating* skills to arrive at acceptable risk mitigations

Unlikely to find these skills in a single person, particularly without professional development

People: Attracting and Keeping Good Security People

- Can be a challenge.
- Focus on the intangibles:
  - Emphasize the mission
  - Relaxed work culture
  - Benefits package - free tuition? better PTO?
  - Community - academic culture and beautiful college towns
  - Academic opportunities and prestige

Services and Tools

- Give careful consideration to the following areas:
  - Characteristics of the product and possible emergent security concerns
  - Service expected from the provider
  - Resources the one must allocate to use the product
- Focus on product vendors and services that are already:
  - Following security best practices relative to their area of focus
  - Communicative and responsive to project-specific security concerns
  - Have procedures for mitigating emergent security issues.
- How you manage these relationships has a substantial effect on the risks and costs associated with information security.

Beware of shiny objects

Examples:

- Sophisticated log collection and analysis software
- Fancy firewalls (or firewall managers!) with advanced capabilities
- IDS/IPS software that generates alerts upon seeing "suspicious activity"

Staff and training resources required are significant

Q&A

Blink twice if you feel very budget constrained.

3.d. Controls

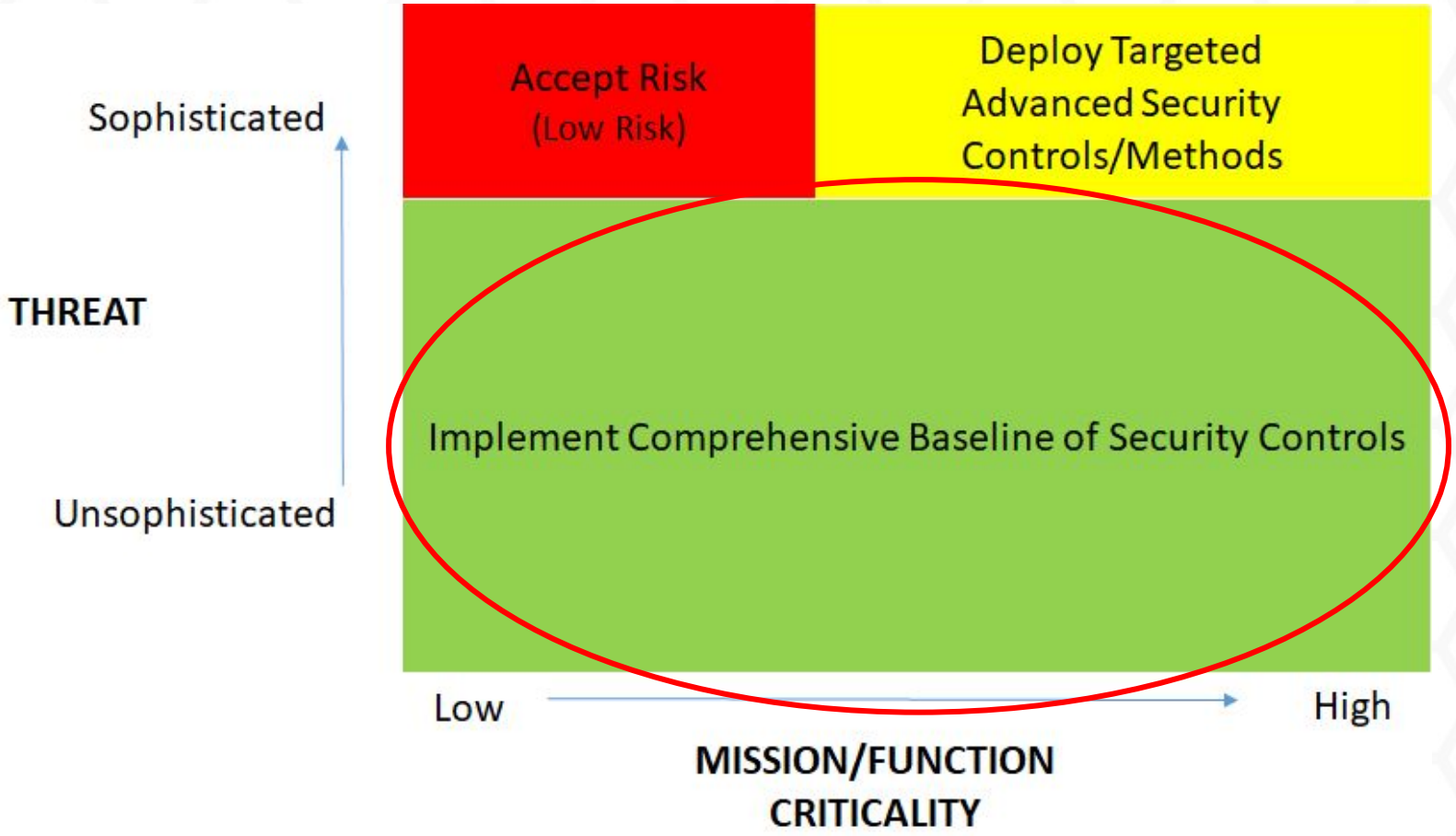
Defining Controls …

Security controls are safeguards or countermeasures to avoid, detect, counteract, or minimize security risks to physical property, information, computer systems, or other assets.

https://en.wikipedia.org/wiki/Security_controls

Controls:
Selecting a Baseline Control Set

Select reasonably scoped, prioritized, and evidence-based baseline control set



Remember the Principles

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

Good Baseline Control Sets

Not all are created equal -- we'll talk about a couple of NIST control sets in a minute (SP 800-53 and SP 800-171). For now, let's look at:

Center for Internet Security (CIS)

- CIS Controls v7

Australian Signals Directorate (ASD)

- ASD Essential Eight

Good Baseline Control Sets

CIS Controls (aka/fka Critical Security Controls, SANS Top 20)

- Prioritized!!! (*See, esp.*, Pescatore, Back to Basics: Focus on the First Six CIS Critical Security Controls)
- Developed in a diverse, practitioner heavy environment. *E.g.*, NSA involved. (See, https://www.sans.org/critical-security-controls/history)
- Updated frequently.
- Testable and provable. (The plaintiffs bar and regulators will prefer this. So will technologists, engineers, and scientists.)
- The CIS Controls have the potential to become the *de facto* legal standard of "reasonable security" nationally.

The First Six (CIS Controls v7)

1: Inventory of Authorized and Unauthorized Devices

2: Inventory of Authorized and Unauthorized Software

3: Continuous Vulnerability Assessment and Remediation

4: Controlled Use of Administrative Privileges

5: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers

6: Maintenance, Monitoring, and Analysis of Audit Logs

Alternative Baseline Control Set

ASD Essential Eight

- Based on systematic study of actual attacks and breaches!!
- Controls selected are those that would have prevented the most breaches
- There are only 8!!! (or potentially 4)
- Prioritized by how many breaches the control would have stopped
- Clear implementation guidance

ASD Essential 8 / CIS v7 Crosswalk

Application Whitelisting

CIS 2.7: Inventory of authorized and unauthorized software: Application Whitelisting

Disable untrusted MS Office Macros (less important for science?)

CIS 2.7: Inventory of authorized and unauthorized software: Application Whitelisting

Patch Applications

CIS 3.5: Continuous vulnerability assessment & remediation: Deploy automated patch mgnt

User Application Hardening

CIS 5.2: Secure configurations for hardware and software: Maintain secure images

Black = Original Top 4; Orange = new additions

ASD Essential 8 / CIS v7 Crosswalk

Restrict Admin Privileges

CIS 4.1: Controlled use of admin privileges: Maintain inventory of admin accounts
CIS 4.3: Controlled use of admin privileges: Ensure appropriate use of admin accounts

Multi-factor Authentication

CIS 4.5: Controlled use of admin privileges: Use multi-factor authentication for admin access
CIS 16.3: Account monitoring and control: Require multi-factor authentication

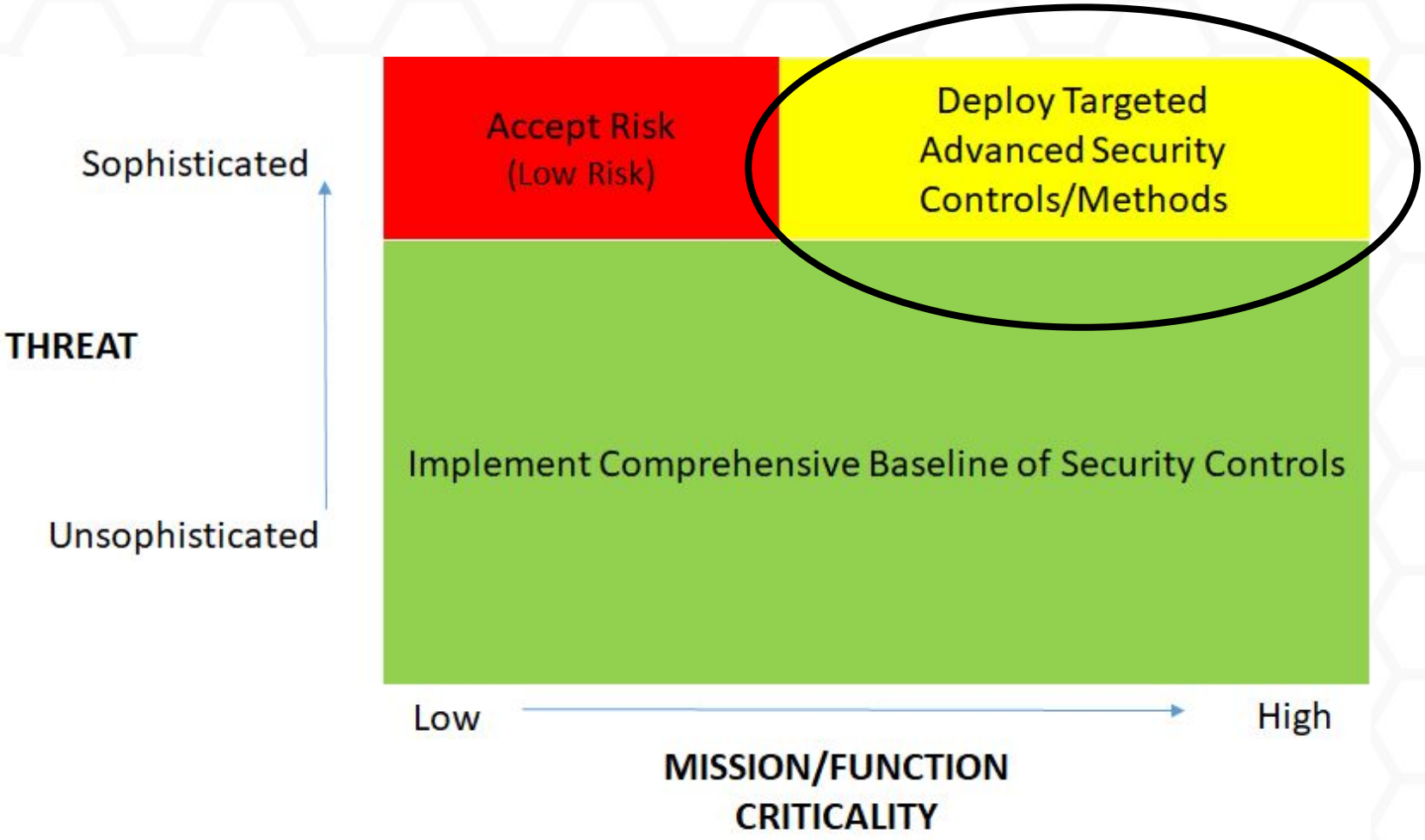
Patch Operating Systems

CIS 5.2: Secure configurations for hardware and software: Maintain secure images
CIS 3.4: Continuous vulnerability assessment & remediation: Deploy operating system automated patch management

Daily Backup of Important Data

CIS 10.1: Data recovery capability: Ensure regular automated backups

Add specialized controls as appropriate



What are the “specials”?

- Secure scientific data and data flows.
- Industrial Control (ICS) and Supervisory Control and Data Acquisition (SCADA) system security.
- Identity management for distributed science communities.
- Non-facility device access to facility networks and data.
- Physical and environmental security.
- Secure software development.

Controls:
Using a Baseline Control Set

Use cybersecurity principles in selecting specific controls

Comprehensivity, Opportunity, Rigor, and Proportionality

Comprehensivity. The control set is a start, not an end. Some controls may be relevant only to certain data flows or systems. Likely will not sufficiently address your specials.

Opportunity. What are you already doing?

Rigor. How do you know?

Proportionality. There are amazing controls that may be effectively impossible to implement.

Example on next slide: Ms. Avila, Bob, and Craig work for a good size research project that operates out of a university. Avila is CIO. Bob is CISO. Craig just has to deal with them.

	A	B	C	D	E	F
1	Control Title	Group	Control Number	Control Description	Asset Type	Security Function
2						
31	**Controlled Use of Administrative Privileges**	**Basic**	**4**	**The processes and tools used to track/control/prevent/correct the use, assignment, and configuration of administrative privileges on computers, networks, and applications.**		
32			4.1	Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.	Users	Detect

G	H	I	J
Relevant?	Status of Implementation	Assessment	Notes
Yes, No, Partial. Some ctrls are clearly relevant. Some may be clearly irrelevant to our environment. Some may be partially relevant. For "no" and "partial," include some prose as to why.	*Prose. Include enough detail that a decision maker can read the control description and the status and be able to make a judgement for the Assessment column, or at least be able to ask intelligent questions. E.g., "Implementation XXXX is in place. We do not do YYYY. The risks associated with not doing YYYY are mitigated by ZZZZ."*	*This is where the decision maker identifies whether the current state is satisfactory, acceptable, unacceptable, or unacceptable and urgently in need of attention*	*There's always notes column, so...*
	See the following descriptions at the 4.X level.		
Yes.	We use a manual, spreadsheet-based process instead. I confirmed Craig maintains that spreadsheet in Google Drive. We explored this last year, but it didn't make the budget. - Respectfully, Your Loyal CISO, Bob	3-Unacceptable	A good automated tool would save us on Craig's labor, even though he's doing a great job maintaining this. I'm marking as unacceptable at this time and teeing up for the next round of budgeting. - Sincerely, Avila

… and, then give people some freedom to innovate and respond to your mission, your dynamic environment, and your specials.

Special Topic

NIST's 3 Control Sets

NIST SP 800-53

- Initially developed in conjunction with FISMA 2002
- Since 2005, has gone through a number of revisions
- Is not meant to be a compliance regime, but has been treated that way by auditors
  - Always allowed for compensating controls and mitigations
- Groups “C I A” requirements at the same level
  - Low, Moderate, High
- Version 5 Draft published in 2017, Final in late 2018

NIST SP 800-53 V5

- Controls in 20 categories described in 260+ pages
- Applicable to federal and non-federal organizations
- Still organized alphabetically, not by priority (*e.g.*, security planning that describes selecting baseline controls is 150 pages into the Controls section)
- Couched in bureaucratic language, difficult to read …

NIST SP 800-53 V5 language example

"Security and privacy plans contain sufficient information (including the specification of parameter values for assignment and selection statements either explicitly or by reference) to enable a design and implementation that is unambiguously compliant with the intent of the plans and subsequent determinations of risk to organizational operations and assets, individuals, other organizations, and the Nation if the plan is implemented as intended. Organizations can also apply tailoring guidance to the control baselines in Appendix D to develop overlays for community-wide use or to address specialized requirements, technologies, missions, business applications, or environments of operation." p. 165

NIST SP 800-53 V5: Bottom Line

Is this your go-to control set?

Absolutely not. Not well-prioritized or reasonably scoped. Not evidence-based.

What to do?

Resist. Only adopt and utilize if you absolutely must.

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/privacy requirements.
- It is a *guidance* document to help implement the executive order.
- It *does not* apply directly to non-federal entities but may be incorporated into contracts, cooperative agreements, or grants.

NIST SP 800-171

- SP 800-171 *wasn't designed* to be a comprehensive control set.
- It is an attempt to standardize federal regulations for unclassified information. (E.g. privacy laws)
- Mostly focused on confidentiality. In many cases, system availability and data integrity are more important to the science mission.
- Still a compliance regime.

NIST SP 800-171: Bottom Line

Is this your go-to control set?

No. Not reasonably scoped. Not evidence-based.

What to do?

Stay vigilant and aware. Another “do if you have to” thing.

NIST CSF “Framework Core”

Again…. CSF is the least of the evils.

1. Organized by Identify, Protect, Detect, Respond, Recover

2. Mapping to other control sets (including CIS Controls)… hooray!!!

NIST CSF “Framework Core”

Is this your go-to control set?

Not really. Still overbroad. Still not prioritized.

What to do?

Use as a *reference*, but focus on the CIS Controls

Don’t you think that was a lot about NIST?

Guilty.

Q&A

4. Operations

Even with Controls “in place” …

Training: Communicating responsibilities

Personnel and Users on Internal Network:

- "Cyber Hygiene"

  "It is the online analogue of personal hygiene, and encapsulates the daily routines, occasional checks and general behaviours required to maintain a user's online "health" (security)" - Wikipedia
- Specific policies that impact their job
- When and where to get help or ask a question

Outside Users:

- AUP (Acceptable Use Policy)

Training (and Professional Development): Cybersecurity staff

Conferences: You're here!; https://www.tripwire.com/state-of-security/featured/top-17-information-security-conferences-2018/; https://www.itspmagazine.com/event-listings/#events-list

Podcasts: https://solutionsreview.com/identity-management/twenty-cybersecurity-podcasts-you-should-be-listening-to/

eMail lists: https://trustedci.org/trustedci-email-lists/ ; https://www.defcon.org/html/links/mailing-lists.html

Webinars: https://trustedci.org/webinars/; BrightTalk; Dark Reading; Gartner; CIS

Classes: SANS; IT ProTV; Coursera

Continuous Monitoring

- Threat monitoring
  - SANS Internet Storm Center https://isc.sans.org/ ;
  - US-CERT;
  - Twitter: @USCERT_gov and @SANSInstitute;
- Configuration and Vulnerability Management
  - OS and application software checked that current, patched versions are installed and securely configured (CIS Controls 3 and 5)
- Log collection and analysis (CIS Control 6)
  - Logs from devices provide data about attacks
  - Many management tools are available; also external monitoring services

Incident Response

- Develop and communicate a plan of action
  - For compromised desktop, server, network
- Include a communication plan
  - Who talks to management, media, CERT, etc.
  - What frequency and the kind of information passed on
- Post-mortem analysis and report
  - Root cause analysis
  - Gauge effectiveness of controls
  - Develop remediation plan, if necessary

RULE: Don’t talk to the media

5. Conclusion

Goals of this training

1. Introduce science projects, support organizations, and granting organizations to the Open Science Cybersecurity Framework, a middle path between compliance madness and complete freedom.
2. Provide actionable guidance, resources, and tools that help you get started on or get serious about your cybersecurity program .
3. Add perspective on special issues and challenges for this community.
4. Answer your questions. Hear your concerns.

Open Science Cybersecurity Framework

Mission Alignment - Governance - Resources - Controls

When in doubt, use the 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?")*

What's next for you?

Attend training sessions this afternoon!

- Software Engineering Guide for NSF Science (Sons)
- Compliance 101: HIPAA, FISMA, NIST 800-171, and GDPR (Anurag, Ramsey, Russell)
- Security Log Analysis Training (Krenz)

What's next for Trusted CI?

Open Science Cybersecurity Framework is coming early 2019. Not just a rewrite, but a complete framework.

Continue to collaborate with the community through the LFST and engagements.

Continue to collaborate with LFO around the LFM.

Much more…. *see*, Von Welch's keynote.

Acknowledgement and Thanks

- National Science Foundation
- Contributors, especially Jim Marsteller, Susan Sons, Scott Russell, Von Welch
- You!

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.

Thanks!

Please fill out the training evaluation!

Kay Avila kayavila@illinois.edu
Bob Cowles bob.cowles@gmail.com
Craig Jackson scjackso@indiana.edu

Bonus Slides

Bonus Topic:
Risk Assessments

DARE to say no. (Defeat Assessment of Risk Everytime.)

What is a risk assessment?

- Frequently listed as procedural control
- NOT the same as *risk management*
- Typical semi-quantitative risk assessment:
  - Gauges the relative magnitude of risk level posed by enumerated hazards
  - Can be focused on one asset or your whole project
  - *See, e.g.*, NIST SP 800-30 rev 1

Bottom line: The deliverable is an *input* to decisions around allocating resources

Ransomware infects the server with all the research data.

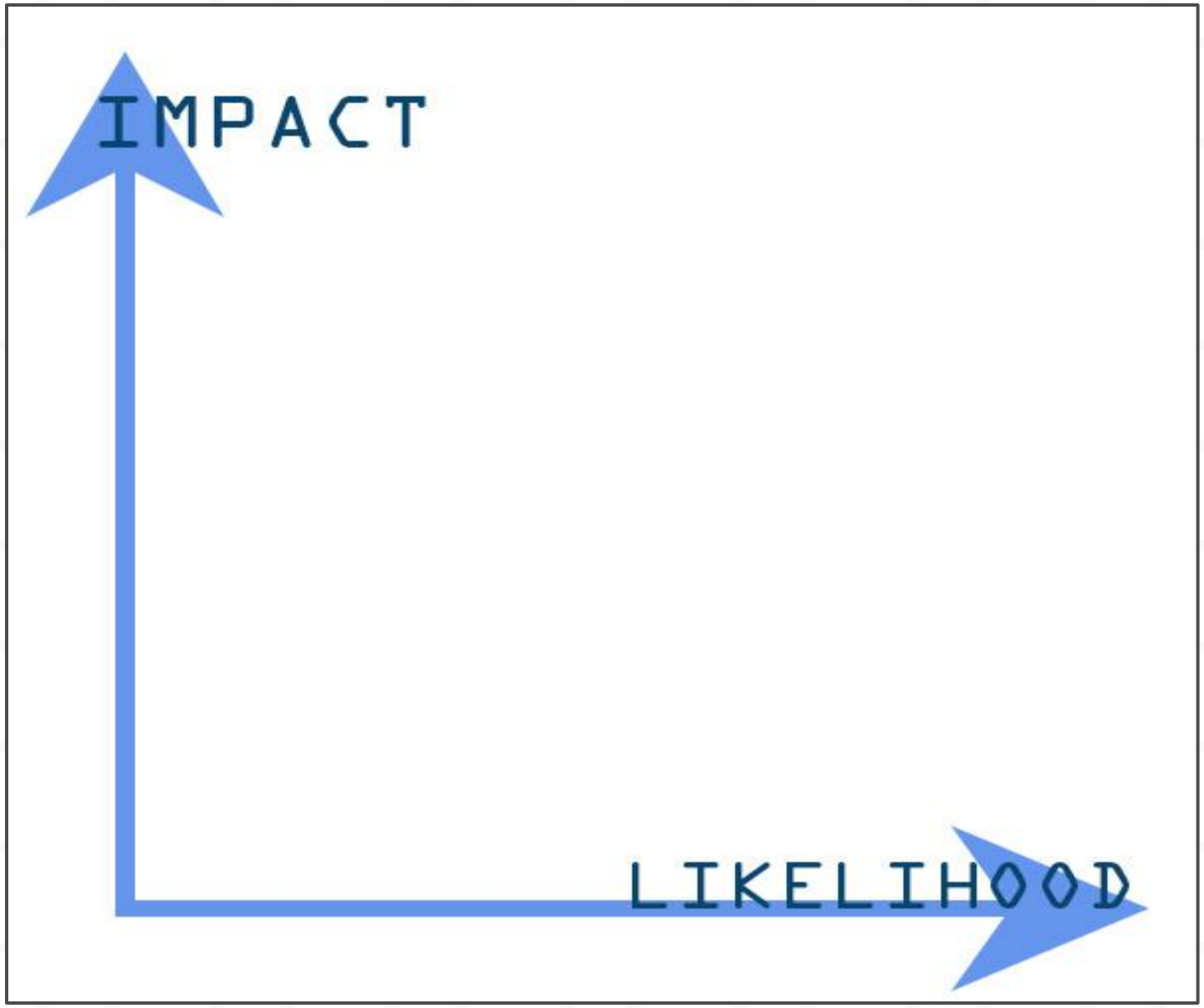
(Estimated) Impact

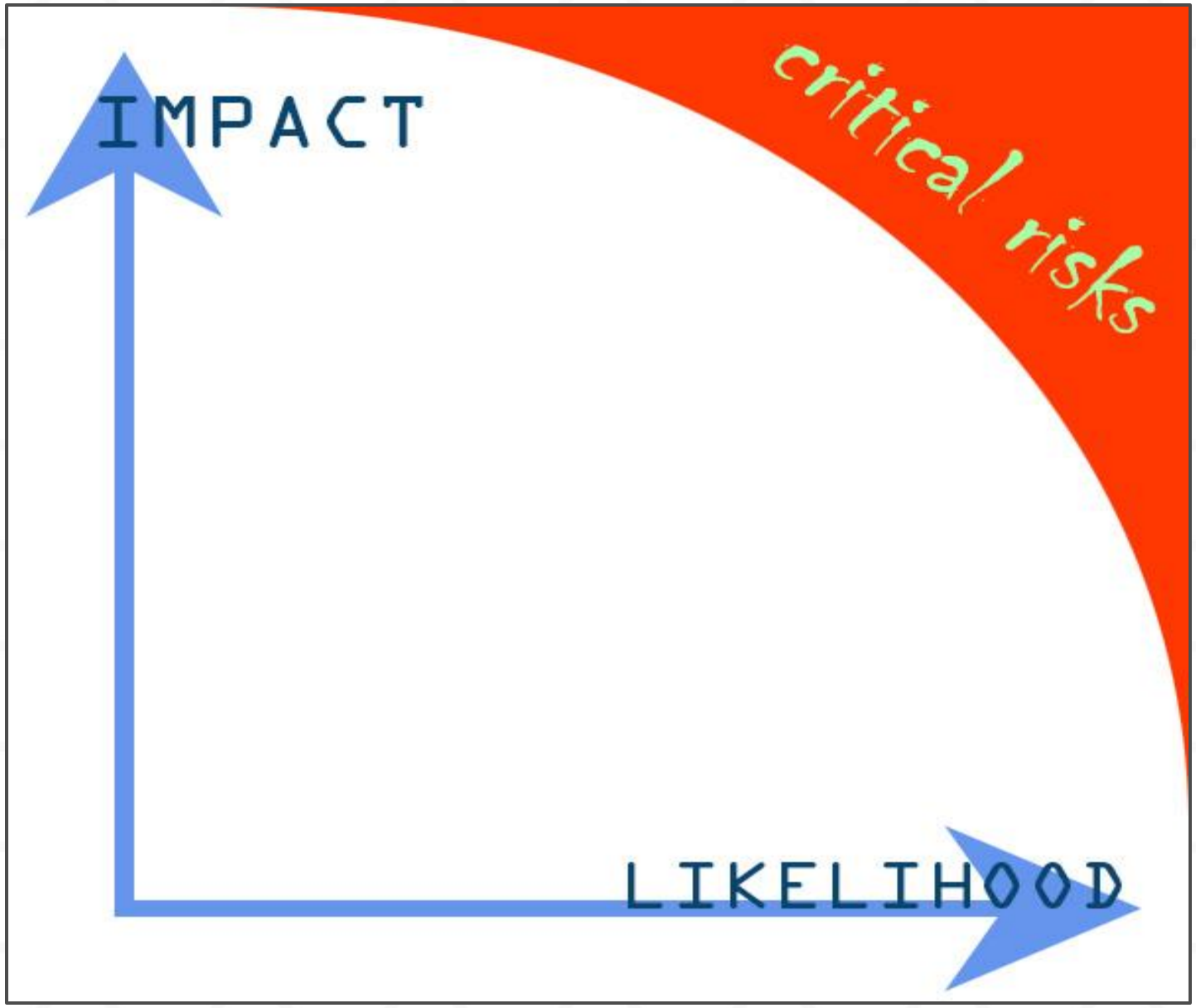
x

(Estimated) Likelihood

=

(Inherent) Risk (Level)


IMPACT
LIKELIHOOD


IMPACT
critical risks
LIKELIHOOD

Benefits of a formal risk assessment?

- Checks a box?
- Forcing function to account for changes in the environment (new threats, new tech, new defenses)
- Surprise findings
- Communication tool

Are risk assessments the only way to allocate resources well?

Absolutely not.

See, again, AFCEA *The Economics of Cybersecurity*

- 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.

Are semi-quantitative risk assessments in the NIST style worth it?

Probably not.

Why not?

- They are expensive.
- They generally produce invalid results particularly wrt “likelihood.”
- They’ll most likely reinforce the fact that you are not and should be doing foundational controls.

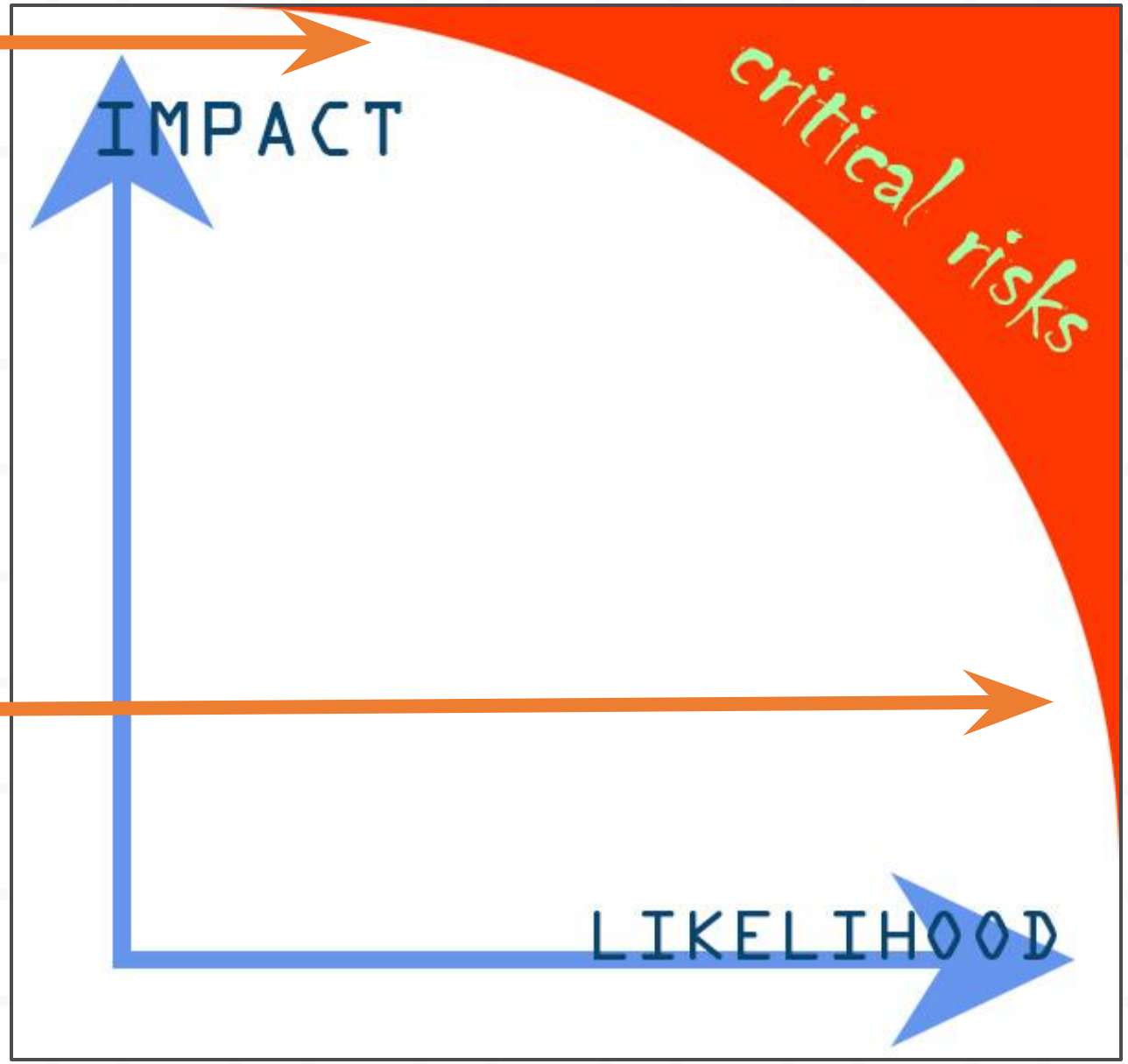
Tips for carrying out semi-quantitative risk assessments (if you just can't help yourself)

- Operationalize your definitions.
  - *Is "extremely likely" a frequency of every day, week, or month?*
- Consistently apply concepts from risk to risk. Don't switch definitions based on the risk!
- Consistently characterize threats events/hazards; include a set of common elements in each description. (Or, use a catalogue; see Appendices E and F of SP 800-30)
- Solicit estimates from multiple sources / validation.
- We have a relatively simple table you can use. *trustedci.org/guide*

Our Risk Assessment Recommendations

- Take an asset-based approach (particularly if your project and/or cyber program are new).
- Focus on your most critical assets and data flows.
- Get the pillars and basic controls in place.
- Consider using the Open Science Cyber Risk Profile. https://trustedci.org/oscrp/
- Look for critical risks, particularly black swans and grey pigeons.

Black Swans



Gray Pigeons

Q&A

Anyone want to share experience with risk assessments?

4. Operations

Operations: Outline

- Are Policies and Controls enough?
- Training: Communicating the Program
- Continuous Monitoring
- Incident Response

With policies and controls in place, are we done?


GATE


AUTHORIZED
PERSONNEL
ONLY


AUTHORIZED
PERSONNEL
ONLY
GATE

Operations:
Training: Communicating the Program

Some people will care about security

..and what about everybody else? Theoretically, everyone is in favor of security (so long as it doesn't get in their way)

Approaches to generating buy-in

- **Top-down**: funding agency requirements, specter of consequences
- **Bottom-up**: they don't want to fail; you're there to help them succeed

Providing information only part of the job

Training is best:

1. In person
2. Personable
3. Make it relevant
4. Don’t just drone on - Sell it!

Everyday experiences will teach more than any training.
What is it teaching them?

Operations:
Continuous Monitoring

Beware of Shadow IT

- Shadow IT - What is it?
- Projects conducted out of policy compliance and without oversight from central IT or cybersecurity
  - Use of cloud for computational or data storage services outside of support structure
  - Includes “critical server” located under Joe’s desk
  - Tradeoff with rapid, agile development
  - Surprise turnover to central IT on deployment
- Identify the renegades and work with them

Operations:
Incident Response

Incident Response Plans

- A determined attacker will succeed and there are many places to hide
- If you are on the Internet, then you are compromised -- the problem is to find them and recover to a “good place”
- Create a general plan based on “PDCA” or “OODA” loops (see Wikipedia articles for explanation)

DON’T PANIC

Douglas Adams, HHGTTG

Incident Response External Resources?

- Your Internet Service Provider
- Parent institution
- Peer organizations
- Incident response contractors
- REN-ISAC
- Your local FBI field office
- Trusted CI

Provide guardrails, not barriers