Developing Cybersecurity Programs for NSF Projects

Center for Trustworthy Scientific Cyberinfrastructure
Bob Cowles, Craig Jackson, Jim Marsteller, Susan Sons

2015 NSF Cybersecurity Summit
August 17, 2015

CTSC

Wireless Access Point:

WestinConference

Super Secret Access Code:

WestinConference

CTSC

Outline

1. Introduction & Overview
2. Establishing a Cybersecurity Program
3. Policy Development
4. Putting It To Work
5. The Daily Joy
6. Keeping Your Program Healthy

CTSC

1.
Introduction & Overview

Training Overview

- Morning:
  - Presenters: Jim Marsteller, Susan Sons, Craig Jackson, Bob Cowles.
  - Q&A period at the end of each section, but Q's are always welcome
- Afternoon:
  - Deep Dives

Will frequently refer to documents at:
trustedci.org/guide

CTSC

Goals of this Training:

1. Introduce PIs and managers of NSF LFs and CI Projects to a concise guide for developing and evolving a cybersecurity program that is tailored to the needs for our community.

2. Elicit discussion and feedback on the same.

Some notes about terminology:

1. We use “information security” and “cybersecurity” more or less interchangeably. We often prefer the former, but have gotten trapped in the cybereverything.

2. If we throw out a term that you don’t understand, please stop us!

How this happened

CTSC

How is the guide different?

1. Authored with a CI perspective
2. Contributions and critique from LF/CI community (TrustedCI Forum, DKIST)
3. Lighter than FISMA/NIST SPs
4. Heavier than, *e.g.*, FCC's small business policy creation tool or NISTIR 7621 *Small Business Information Security: The Fundamentals*
5. Publicly available and free to use (unlike, *e.g.*, ISO)
6. Templates, templates, templates!!!
7. Community-driven approach - Community to contribute to the evolution of the guide

CTSC

So, what is a cybersecurity "program?"

"A cybersecurity program is a structured approach to develop, implement, and maintain an organizational environment conducive to appropriate information security and levels of information-related risk. Cybersecurity programs entail ongoing activities to address relevant policies and procedures; technology and mitigations; and training and awareness. Cybersecurity programs are scoped to the key assets, resources, and lifespan of organizations." - CTSC

CTSC

Why is a cybersecurity program important?

- Underlies trustworthy science - Maintaining the trust of scientists and the public in the CI, data and science.
- Prevents infrastructure from being used against others.
- Addresses information security requirements as defined in NSF cooperative agreements.
- Enables collaboration by supporting trust.

What are the components of a comprehensive program?

1. If you've got it, see your Cooperative Agreement.

2. See the NIST Framework or any number of cybersecurity maturity models.
   The 22 Framework Core "Categories" are a great place to get a feel.

Table 1: Function and Category Unique Identifiers

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
PR	Protect	PR.AC	Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

CTSC

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. (*See*, recent IRNC solicitation.)

CA-FATC LF Article 58 and CA-FATC FFRDC Article 61:

"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's organization as part of the organization's IT security program, in place or planned, to protect research and education activities in support of the award."

CA-FATC LF Article 58 and CA-FATC FFRDC Article 61:

"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 institution'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 subawardees, subcontractors, researchers and others who will have access to the systems employed in support of this award."

CA-FATC LF Article 58 and CA-FATC FFRDC Article 61:

"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."

“Roles and Responsibilities”

CTSC Resources:

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

“Risk Assessment”

CTSC Resources:

- *Information Asset Inventory*
- *Risk Assessment Table*

“Technical, Administrative, Physical Safeguards”

CTSC 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”

CTSC Resources:

- *Information Security Training and Awareness Policy*
- *CTSC “Cyber Hygiene” Information Security Training Slide Deck*

“Notification Procedures”

CTSC Resources:

- *Incident Response Policy and Procedures*

"Evaluation Criteria"

CTSC Resources:

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

"Appropriate Security Measures for Subawardees/Subcontractors, Researchers and Others"

CTSC Resources:

- *Acceptable Use Policy (AUP)*

CTSC

Q&A

2.
Establishing a Cybersecurity Program

Establishing a Cybersecurity Program

a. Core Processes and Tools

b. Risk-Based Approaches

c. Selecting Baseline Controls

d. The Role of Risk Assessments

CTSC Cybersecurity Program Processes & Core Tools

Importance of Project Leadership

PIs have the ultimate responsibility for ensuring the project has an effective information security program

- Promote the importance of a cybersecurity program
- Assigning security responsibilities
- Determine acceptable levels of risk
- Support cybersecurity program

Roles and Responsibilities

- Senior Management
  - Takes active role in allocating adequate resources, address program governance, accept residual risk, and follow information security policies
- Asset Owner
  - Understands risks to the asset and ensures appropriate controls are in place while the assets are being developed, produced, maintained, and used
- Chief Information Security Officer (CISO)
  - Knowledgeable in information security, understand how information assets relate to the organization's mission, effectively communicate the issues and the tradeoffs; empowered as a decision-maker and key stakeholder where expert and timely action are required to protect organizational interests

Project 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.

Project Relationships

You are not alone

CI Projects are becoming increasingly distributed.

Multi-institutional, international, interdisciplinary but highly interconnected. Virtual project teams are commonplace.

While this can create challenges, it also creates opportunity.

Challenges of CI projects

- 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

Opportunities in CI Projects
"I've got your back"

- Collective knowledge a of distributed team can be a resource of support. "Has anyone seen this unusual network traffic?"
- Improve detection ability and response times by sharing event information. "Mass scanning from IP address 201.234.178.62, suggest blocking"
- Ad-hoc support in times of need.

CTSC

This slide intentionally left blank.

Risk!

CTSC

Risk-based approaches

- NIST 800 Series / FISMA*
- HIPAA Security Rule*
- DIARMF*…. even DOD is going there; DIACAP is out!
- NIST Framework for Improving Critical Infrastructure Cybersecurity
- ISO 27005
- COBIT

* *blended into compliance regimes*

CTSC

Why risk management? Flexibility.

- pure compliance or rule-based approaches are generally inappropriate for infosec

  fast-changing, relatively new,

  relatively low risk (for now)
- well-suited for organizations with limited resources and time
- good for situations where the type of risk is difficult to insure against or the "insured" is hard to identify
- allows for mitigation, transfer, avoidance, and acceptance of risk

Why do we find the need to sell you on risk management?

Guesses?

Craig's answer: It's risky.

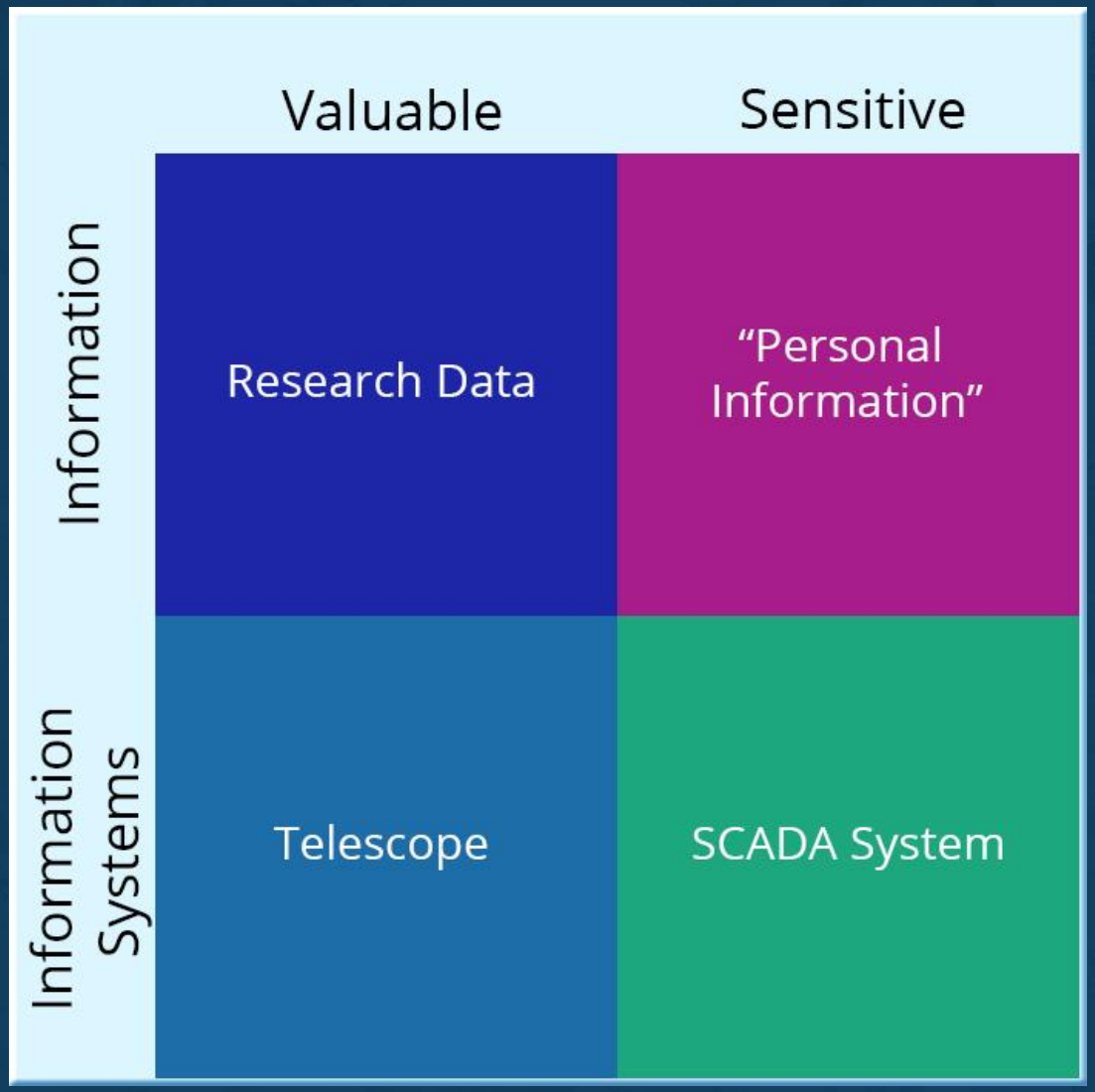
1. *Ownership*
2. *Effort*
3. *Time*
4. *Thought*
5. *There are lots of well-established best practices out there!*

Where to begin?

If I buy into a risk based approach, then what?

As we'll discuss repeatedly, there is *not just one answer to that question*, but identifying and documenting your information assets, as well as understanding their value and/or sensitivity is a wildly helpful step that can be overlooked or underemphasized.

“Information Assets”



Tips for Identifying Information Assets

1. Create and maintain solid documentation of what is actually there.
   a. Information Asset Inventory
   b. A solid basis for selecting controls, conducting RAs; an investment in continuity of the program.
2. Start with your information inventory (*vs* information systems) and capturing data flows.
3. Think in terms of types of information and information systems; get more detailed as needed.
4. Take the opportunity to get a handle on the security objectives for those assets.

1.2 Type of Information

⇒ *Enter a description of this information type here. It should be specific enough that someone who was handed a disk full of data can easily determine whether the data they have belongs to this classification or not. In the table below, you'll list information that's part of this set.*

Asset Name	Short Description	Owner	Asset Detail
Insert a short name to unambiguously identify asset	*Describe the asset. Unless there's a referenced asset detail, this should include where it is and how it's accessed.*	*Who is responsible for this asset?*	*Where is there more information about this asset?*

Confidentiality:
Integrity:
Availability:

Yes, we've got a template for that.

CTSC

Information Asset Details:

- What's included in this set?
- Why do we have it? Where is it coming from, and what do we use it for?
- How is this set 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?

CTSC

The '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.

See, 44 U.S.C. 3542(b) and FIPS 199

Project Mission & Interests

'CIA' Security Objectives

Controls

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.

The process for info systems is similar:

2.2 Type of Information System

⇒ *Enter a description of this system type here. It should be specific enough that someone who was handed a disk full of data can easily determine whether the data they have belongs to this classification or not. In the table below, you'll list information that's part of this set.*

Asset Name	Short Description	Owner	Asset Detail
Insert a short name, may be descriptive or may be the system hostname.	Describe the asset. Type of equipment, its function, etc. For hardware, include model and serial number when available.	Who is responsible for this asset?	Where is this asset documented in more detail?

Confidentiality:
Integrity:
Availability:

CTSC

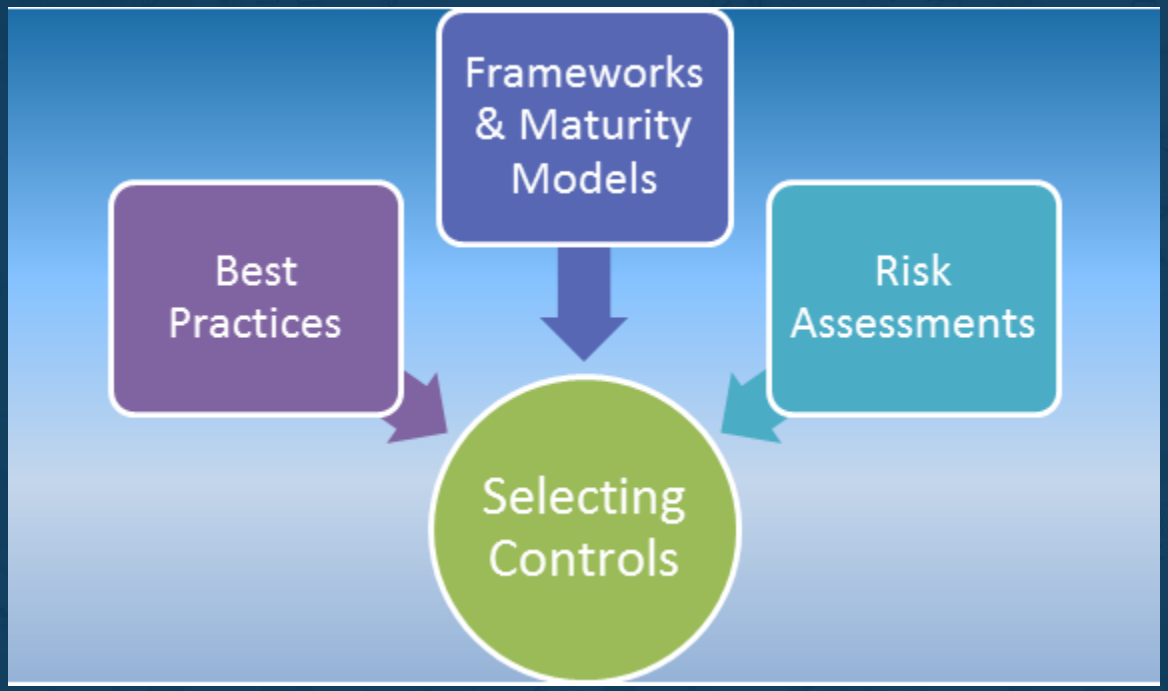
Details on information systems:

- Hardware specs & serials (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

Next Up:

Selecting Baseline Controls



All these can feed into selecting controls,
but we need to talk about selecting baseline controls.

CTSC

Selecting Baseline Controls: You have options!

- Concise Best Practices Guides
  - SANS/NSA/CSIS *Critical Security Controls*
  - CTSC's *Securing Commodity IT*
- Extensive Best Practices Guides
  - 800-53 rev 4
  - ISO 27002
- Risk Assessment Results
  - Lots more on RA's later
- Program Evaluation Frameworks / Maturity Models
- *What to choose?...*

CTSC

Project timeline and lifespan are important

CTSC

Best Practices Guides

- Concise Best Practices Guides
  - SANS *Critical Security Controls*
  - CTSC's *Securing Commodity IT*
- Extensive Best Practices Guides
  - NIST SP 800-53 rev 4

Program Evaluation Frameworks & Maturity Models

- Overarching best practices view of a program

- *E.g.*,
  - NIST Framework for Improving Critical Infrastructure Cybersecurity
  - Booz Allen Cyber Operations Maturity Framework
  - Higher Education Information Security Council (HEISC) Information Security Program Assessment Tool
  - Electricity Subsector Cybersecurity Capability Maturity Model (ES-C2M2)

Q&A

The Role of Risk Assessments

- NOT the same as *risk management*
- A flexible tool: gauging the relative magnitude of risks
- Can be focused on one asset or your whole project
- An *input* to decisions around resource allocation
- An opportunity to gauge control effectiveness
- *E.g.*, NIST SP 800-30

(Estimated) Impact

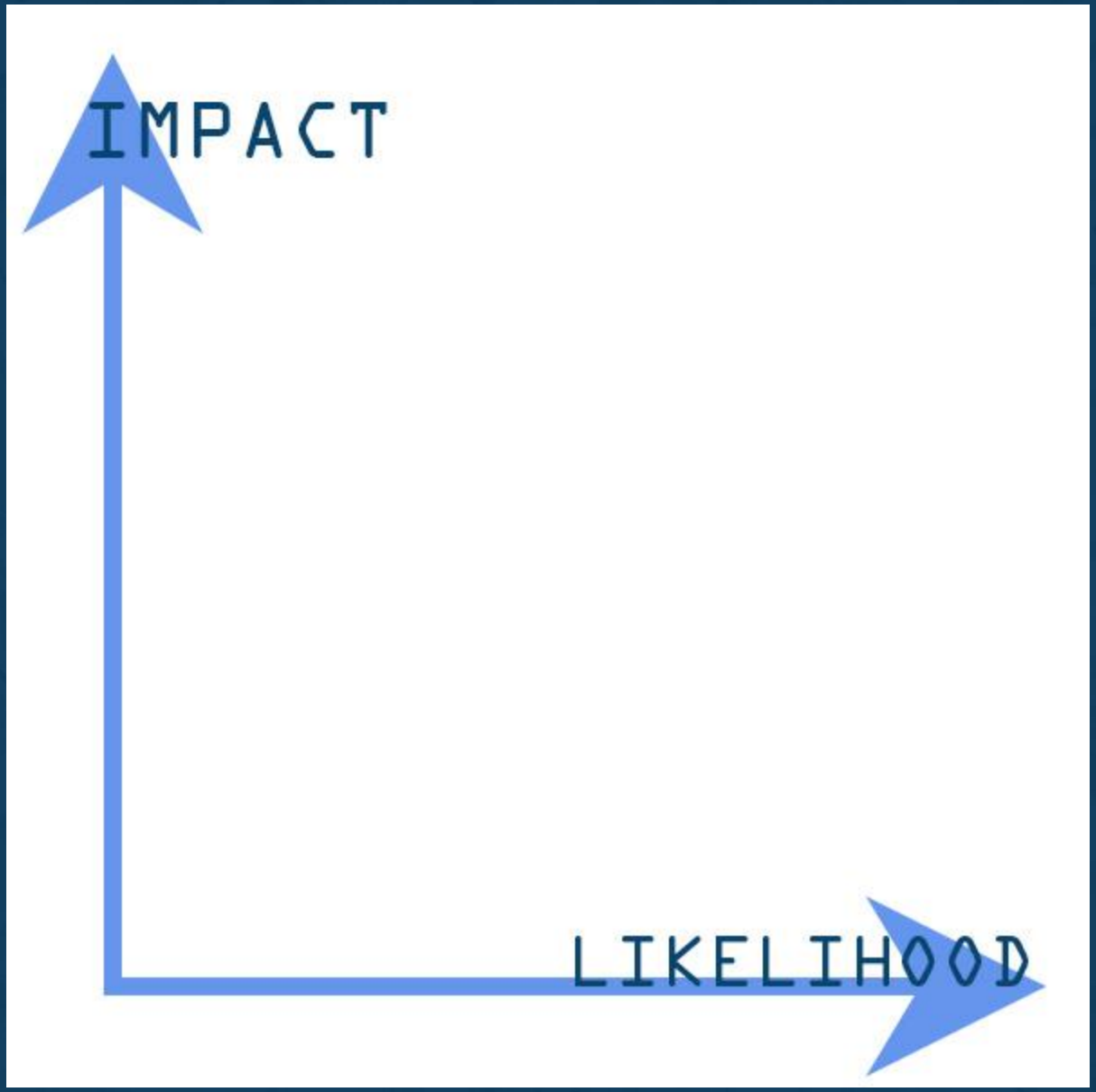
x

(Estimated) Likelihood

=

(Inherent) Risk (Level)

CTSC


IMPACT
LIKELIHOOD

Risk Assessment is fundamentally….

About matching available effort and resources to feasible threats in order to achieve acceptable levels of risk.

Crown jewels +
Likely threat event +
No Controls =
We've got a problem

Commodity IT + Controls are cheap/easy +
No Controls =
We've got an easy win

Risk Assessment Recommendations

1. Consider holding off on a formal or extensive risk assessment, and first consider the scope, structure, and roadmap for your program.
2. Consider lightweight or heavyweight, targeted or comprehensive assessments based on where you are in your project lifespan and available resources
3. Take an asset-based approach (particularly if your project and/or cyber program are new):

   Understanding the value and sensitivity (and location and access controls) of your information and information systems is an early step to any risk assessment

Kickstarting a program

A couple case examples...

CTSC

Case 1… a new project, kickstarting a program

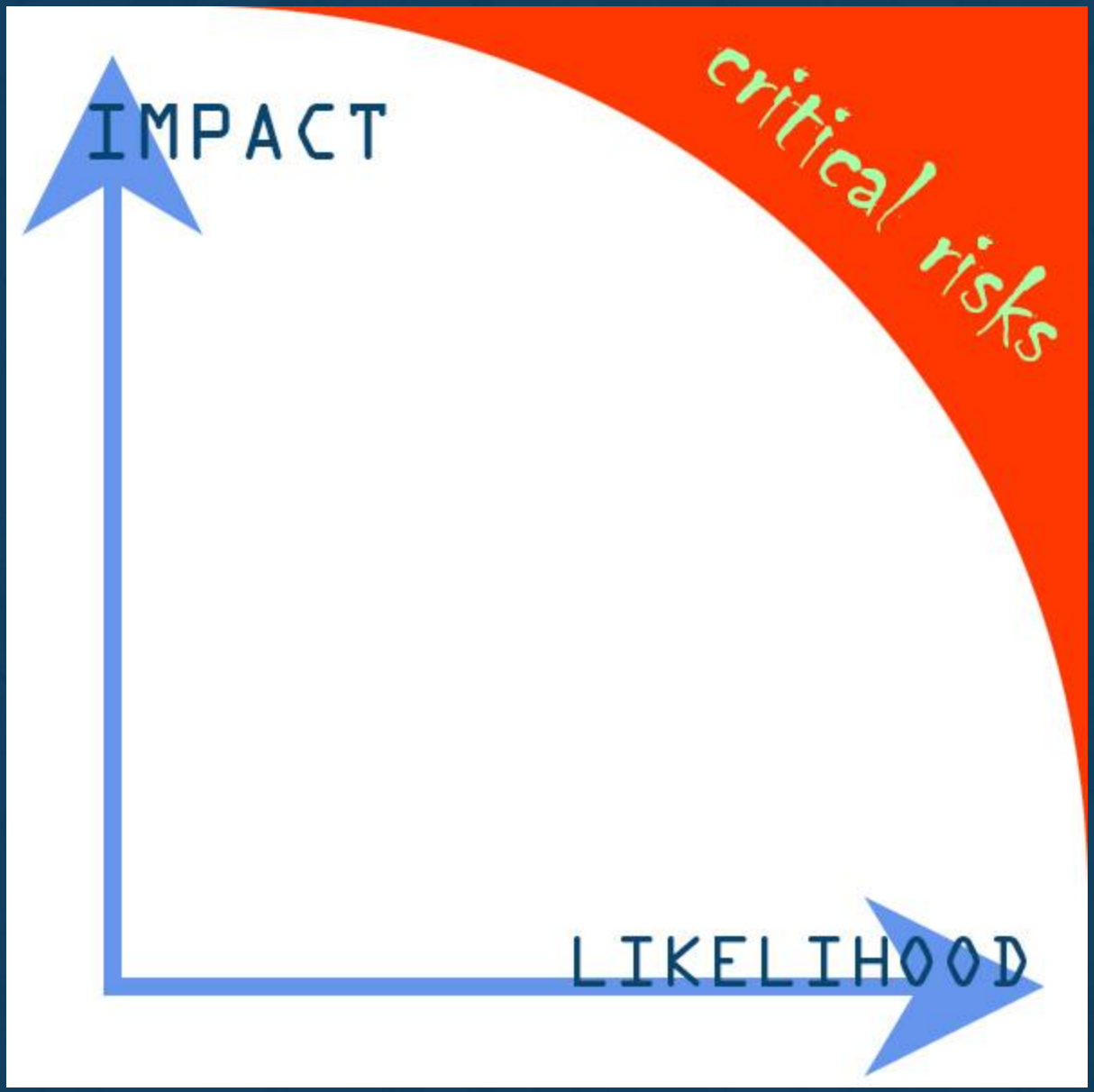
- Identify your information assets (information + information systems), and know which are mission critical and sensitive.
- Identify & implement best practices. *Society has done the risk assessment for you!*
  - If no best practices exist / too complex to identify or implement / want to make sure you've got the critical stuff covered…. get help.
- Pick a maturity model or use the NIST Framework to envision your program. How sophisticated can you afford to be?

CTSC

Case 2… a not-so-new project, kickstarting a program

1. Identify Critical Risks
   a. "Cybercheckup" - Identifying holes in the ship.
   b. *Black swans*. Reduce impact / contingency planning.
   c. *Grey pigeons*. High-likelihood/frequency incidents. Reduce frequency and aggregate impact.
   d. *Low-hanging fruit*. May be outside critical zone, but cheap, easy wins.
2. Select Targeted Controls
   a. Again, best practices!
3. Identify, Protect, Detect, Respond, Recover… remember its not all about prevention.

Pigeon Credit - Ian Burt - CC by 2.0


IMPACT
critical risks
LIKELIHOOD

That said…. Let's talk a bit more about our approach to formal risk assessments, tips, and tools.

Benefits of a Formal Risk Assessment

- Assist a project with identifying gaps in a security program
- Output of a RA can be used to develop a cybersecurity plan (mitigation plan and ownership)
- More advanced designs can be used to evaluate control effectiveness

13	Risk	assets, individuals, other organizations, or the Nation) from the threat event. (Task 2-5; Table H-1; Table H-2; Table H-3; Table H-4; Table I-5.) Determine the level of risk as a combination of likelihood and impact. (Task 2-6; Table I-1; Table I-2; Table I-3; Table I-5.)

TABLE I-5: TEMPLATE – ADVERSARIAL RISK

1	2	3	4	5	6	7	8	9	10	11	12	13
Threat Event	Threat Sources	Threat Source Characteristics			Relevance	Likelihood of Attack Initiation	Vulnerabilities and Predisposing Conditions	Severity and Pervasiveness	Likelihood Initiated Attack Succeeds	Overall Likelihood	Level of Impact	Risk
		Capability	Intent	Targeting								

NIST SP 800-30 rev 1, Appendix I, p.I-3

CTSC

TABLE D-2: TAXONOMY OF THREAT SOURCES

Type of Threat Source	Description	Characteristics

ADVERSARIAL
- Individual
  - Outsider
  - Insider
  - Trusted Insider
  - Privileged Insider
- Group
  - Ad hoc
  - Established
- Organization
  - Competitor
  - Supplier
  - Partner
  - Customer
- Nation-State
	Individuals, groups, organizations, or states that seek to exploit the organization's dependence on cyber resources (i.e., information in electronic form, information and communications technologies, and the communications and information-handling capabilities provided by those technologies).	Capability, Intent, Targeting

ACCIDENTAL - User - Privileged User/Administrator	Erroneous actions taken by individuals in the course of executing their everyday responsibilities.	Range of effects

STRUCTURAL
- Information Technology (IT) Equipment
  - Storage
  - Processing
  - Communications
  - Display
  - Sensor
  - Controller
- Environmental Controls
  - Temperature/Humidity Controls
  - Power Supply
- Software
  - Operating System
  - Networking
  - General-Purpose Application
  - Mission-Specific Application
	Failures of equipment, environmental controls, or software due to aging, resource depletion, or other circumstances which exceed expected operating parameters.	Range of effects

ENVIRONMENTAL
- Natural or man-made disaster
  - Fire
  - Flood/Tsunami
  - Windstorm/Tornado
  - Hurricane
  - Earthquake
  - Bombing
  - Overrun
- Unusual Natural Event (e.g., sunspots)
- Infrastructure Failure/Outage
  - Telecommunications
  - Electrical Power
	Natural disasters and failures of critical infrastructures on which the organization depends, but which are outside the control of the organization.
	Note: Natural and man-made disasters can also be characterized in terms of their severity and/or duration. However, because the threat source and the threat event are strongly identified, severity and duration can be included in the description of the threat event (e.g., Category 5 hurricane causes extensive damage to the facilities housing mission-critical systems, making those systems unavailable for three weeks).
		Range of effects

NIST 800-30, Appendix I, Page D-2.

CTSC

Basic InfoSec Risk Management Terms

Asset: Assets are valuable and/or sensitive organizational information and information systems.

Vulnerability: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations and/or stakeholders through an information system via a loss of information security

Basic InfoSec Risk Management Terms

Threat: Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations and/or stakeholders through an information system via a loss of information security.

Control: The management, operational, and technical safeguards or countermeasures prescribed for an information system to protect the confidentiality, integrity, and/or availability of information assets

Characterizing Threats

Use an asset based approach

Asset	Attack Surface	Threat Description	What could go wrong?
Email (Data)	Email Server	A third party exploits a vulnerability or misconfiguration in server to access emails stored on the server or observe them being received or transmitted by the server.	3rd party data we're responsible for protecting is breached; we may have to inform everyone; may have to support mitigating damages, investigation, manage reputation
Email (Server & Service)	Postfix (mail transfer agent)	An attacker could use our mail server to send spam.	Consumes our bandwidth, delays legitimate emails, we (our project or whole parent organization) get blocklisted and can't send email at all until resolved.
Instrument Control System	Web-Based Control Interface	An attacker could exploit the web application we use to remotely turn our instruments' sensors on and off, causing sensors to be turned off or become unavailable when needed.	Loss of valuable sensor telemetry, possibly during a once-in-a-lifetime event.

Characterizing Threats

How does the threat attack the asset?

Asset	Attack Surface	Threat Description	What could go wrong?
Email (Data)	Email Server	A third party exploits a vulnerability or misconfiguration in server to access emails stored on the server or observe them being received or transmitted by the server.	3rd party data we're responsible for protecting is breached; we may have to inform everyone; may have to support mitigating damages, investigation, manage reputation
Email (Server & Service)	Postfix (mail transfer agent)	An attacker could use our mail server to send spam.	Consumes our bandwidth, delays legitimate emails, we (our project or whole parent organization) get blocklisted and can't send email at all until resolved.
Instrument Control System	Web-Based Control Interface	An attacker could exploit the web application we use to remotely turn our instruments' sensors on and off, causing sensors to be turned off or become unavailable when needed.	Loss of valuable sensor telemetry, possibly during a once-in-a-lifetime event.

CTSC

Estimating Impact

Impact measures the degree of potential harm to organizational interests.

Things to consider when estimating impact:

- Asset value
- Asset sensitivity
- Nature of impact (financial, reputation, human harm)
- Cost of response

Estimating Impact

CTSC Risk Assessment Scale:

If the incident were to occur, what would be the potential impact (of a single occurrence)?

5 - Catastrophic

4 - Major

3 - Moderate

2 - Minor

1 - Insignificant

Estimating Impact

5 - Catastrophic

4 - Major

3 - Moderate

2 - Minor

1 - Insignificant

What could go wrong?	Impact	Likelihood	Control Effectiveness	Inherent Risk Level Scale: 1 - 25	Residual Risk Level Scale: 0-25
3rd party data we're responsible for protecting is breached; we may have to inform everyone; may have to support mitigating damages, investigation, manage reputation	3	3	5	**9**	**2**
Consumes our bandwidth, delays legitimate emails, we (our project or whole parent organization) get blocklisted and can't send email at all until resolved.	4	5	3	**20**	**12**
Loss of valuable sensor telemetry, possibly during a once-in-a-lifetime event.	5	2	3	**10**	**6**

CTSC

Estimating Likelihood

What it is: Probability that a vulnerability will be exercised by a threat

Things to consider when estimating likelihood:

- Anticipated frequency (10 year or 100 flood?)
- Motivation, knowledge and capabilities of threat sources
- Specifics of vulnerability (easy/difficult to execute)
- Confidence in performing the estimation

CTSC

Estimating Likelihood

5 - Constant, or extremely frequent
4 - Very frequent
3 - Somewhat frequent
2 - Infrequent
1 - Rarely, if ever

What could go wrong?	Impact	Likelihood	Control Effectiveness	Inherent Risk Level Scale: 1 - 25	Residual Risk Level Scale: 0-25
3rd party data we're responsible for protecting is breached; we may have to inform everyone; may have to support mitigating damages, investigation, manage reputation	3	3	5	**9**	**2**
Consumes our bandwidth, delays legitimate emails, we (our project or whole parent organization) get blocklisted and can't send email at all until resolved.	4	5	3	**20**	**12**
Loss of valuable sensor telemetry, possibly during a once-in-a-lifetime event.	5	2	3	**10**	**6**

CTSC

Estimating Control Effectiveness and Residual Risk

5 - Extremely effective
4 - Very effective
3 - Moderately effective
2 - Minimally effective
1 - Ineffective

What could go wrong?	Impact	Likelihood	Control Effectiveness	Inherent Risk Level Scale: 1 - 25	Residual Risk Level Scale: 0-25
3rd party data we're responsible for protecting is breached; we may have to inform everyone; may have to support mitigating damages, investigation, manage reputation	3	3	5	**9**	**2**
Consumes our bandwidth, delays legitimate emails, we (our project or whole parent organization) get blocklisted and can't send email at all until resolved.	4	5	3	**20**	**12**
Loss of valuable sensor telemetry, possibly during a once-in-a-lifetime event.	5	2	3	**10**	**6**

CTSC

Using the results of the assessment

- If residual risk level is not acceptable, select additional controls to attain acceptable risk level
- Determine action plan and activity owner

Control Effectiveness	Inherent Risk Level Scale: 1 - 25	Residual Risk Level Scale: 0-25	Further Mitigation Warranted?	Action/Mitigation Plan	Mitigation Activity Owner
5	9	2	No	Maintain current practice. Server only allows encrypted connections; all configuration changes are checked by Senior Systems Administrator before going into production; security updates to server software are applied promptly.	Senior Systems Administrator
3	20	12	Yes	Server software is currently kept up to date; administrative access to the server is limited to the local network and requires two-factor authentication. However, users currently don't have to authenticate to the server for sending mail if they have received mail recently. This should be changed so that users' email clients must authenticate each connection.	Senior Systems Administrator
3	10	6	Maybe	Consider 2FA. The control server is behind a firewall, but security could be increased by using two-factor authentication instead of passwords alone, and/or making it accessible only from the VPN.	ISO

Tips for carrying out comprehensive RAs

1. Operationalize your definitions.

   Is "extremely likely" a frequency of every day, week, or month?

2. Consistently apply concepts from risk to risk. Don't switch definitions based on the risk!
3. Consistently characterize threats; include a set of common elements in each description. (Or, use a catalogue; see Appendices E and F of 800-30)
4. Solicit estimations from multiple sources / validation.

CTSC

Q&A

3.
Policy Development

Policy Development

Program formalization is a key step in virtually all maturity models for distinguishing relatively immature programs from relatively mature. Policy development and implementation is necessary for formalization.

Results in:

- Reproducible, communicable, and enforceable processes.
- Artifacts that can be critiqued and evolved.

CTSC

Templates!!!

We will refer to templates found at the following page: http://trustedci.org/guide

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

Policy Development

1. A brief overview of the range of policies
2. Highlight a selection of policies
3. Talk about some tips

Policies we'll highlight

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

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.

- Define rights and responsibilities of all users
- Establishes authority
- 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)

Incident Response Policy

Purpose: Decide and document what to do in the event of a security incident BEFORE on 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)
- Define who is responsible for which decisions
- Lay out response procedures for grey pigeon and black swan events
- Specify when and how response procedures will be tested
- Afternoon IR training available!

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.
- Least privilege principle
- Authentication vs. authorization
- Impacts every control

CTSC

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.
- Input is key…. think general counsel.
- Int'l collaboration can complicate things in a hurry.

Policy Development: Tips, Gotchas

- 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:
  a. Allow policies to be developed and filed away without a formal approval process
  b. Work in a vacuum
  c. Assume you need one of each
  d. Be afraid to take this seriously
  e. Underestimate the power of v2

Q&A

Section 4:
Putting It To Work
Education & Implementation

Who cares?

...and what do I do with everybody else?

CTSC

Inside Users / Personnel:

- “Cyber Hygiene”
  - See this slide deck at http://trustedci.org/guide
- Specific policies that impact their job
- When to get help or ask a question

Outside Users:

- AUP (Acceptable Use Policy)

Training methods matter.

Providing information is only half the job.

Training:

- In person
- Be personable
- Make it relevant
- Sales, not just exposition.

CTSC

The everyday experience will teach your team more than any training you give them.

What is it teaching them?

CTSC

CTSC

Putting it all in place

New Projects:

- Put security practices in place as parts of your project/CI come online.
- You can and should evolve your program over time: don't get stalled trying to do everything at once.
- Focus on hygiene (e.g., best practices) first, and big dangers as they become apparent (grey pigeons and black swans).

Established Projects:

- Documenting your assets may be a big job. Do it anyway.
- Find gaps, then prioritize and fill.
- Implement changes in stages rather than all at once.
- The more you grow, the more you'll want to consider automation.

Section 5:
The Daily Joy of
Operational Security

CTSC


AUTHORIZED
PERSONNEL
ONLY
GATE


GATE

CTSC

CTSC


AUTHORIZED
PERSONNEL
ONLY
GATE

Continuous Monitoring

i.e., Appropriately Frequent Monitoring

- Threat monitoring
  - SANS Internet Storm Center; United States Computer Emergency Response Team (US-CERT); SANS also has a weekly and semi-weekly newsletters
- Configuration and Vulnerability Management
  - OS and application software checked that current, patched versions are installed and securely configured
- Log collection and analysis
  - Logs from devices provide data about attacks
  - Many management tools are available; also external monitoring services

External Resources and Partners

- Your Internet Service Provider
- Parent Institution
- Peer Organizations
- Commercial Security Consultants
- REN-ISAC
- Bro Center of Expertise
- FBI Cyber Crime Unit
- CTSC

Using External Security Sources

- NIST SP 800-35 and SP 800-36 contain advice
- Get insight into what external sources have to offer
  - Balance risks, costs, and benefits
  - Trade-offs: control, resource demands, available expertise
- Clarify expectations
  - Ensure contract service level agreement (SLA), memorandum of understanding (MOU), or other agreement outlines relevant security expectations

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 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

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)

Douglas Adams, HHGTTG

Section 6: Keeping Your Program Healthy

So you've…

…figured out what assets you are protecting.

…taken a look at your risks.

…written policies and procedures.

…trained personnel.

In short, you've made a plan and followed it.

Now What?

Keeping Your Program Healthy Means:

- Keeping security-related overhead low so you won't have to choose between information security and your core mission.
- Testing procedures to make sure they work
  - Incident response is your most important area to test, because when you need it, something has already gone wrong.
- Reviewing policies to ensure that they still fit your project or organization well.
- Risk Assessment, Program Evaluation

Congrats, your job is security.

(and science, and teaching, and mentoring interns, and getting grants, and…)

What should we test and how often should we test it?

CTSC

Q&A

CTSC

Section 7: Conclusion

CTSC Cybersecurity Program Processes & Core Tools

Next steps for our team.

1. Incorporating your feedback and ideas in our training and the Guide.
2. Looking for more opportunities to work through the guide with NSF projects
3. Data Breach Handling Template
4. Information of budgeting for cybersecurity personnel and programs
5. Consider implications of int'l collaboration

CTSC

Q&A

CTSC

Review

1. Introduction & Overview
2. Establishing a Cybersecurity Program
3. Policy Development
4. Putting It To Work
5. The Daily Joy
6. Keeping Your Program Healthy

CTSC

Resources

- Center for Trustworthy Scientific Cyberinfrastructure
  - http://trustedci.org/contact/
  - http://trustedci.org/guide/
  - http://trustedci.org/ctsc-email-lists/
- NIST Cybersecurity Framework
  - http://www.nist.gov/cyberframework/
- NIST Special Publications
  - http://csrc.nist.gov/publications/PubsSPs.html
- Critical Security Controls
  - https://www.sans.org/critical-security-controls/

Acknowledgements & Thanks

- National Science Foundation
- Bret Goodrich & DKIST / NSO
- Contributors & Commenters
- You!

This document/presentation is a product of the Center for Trustworthy Scientific Cyberinfrastructure (CTSC). CTSC is supported by the National Science Foundation under Grant Number OCI-1234408. 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!

Let’s eat.

CTSC

Welcome back!

CTSC

Afternoon Sessions

1. Goals:
   a. More opportunity for inter-project sharing.
   b. Offer guidance on this identified challenges.
   c. Unearth issues where there is a lot of resonance across the community. (Findings for the summit report.)
2. Format:
   a. Facilitated discussion interlaced with expert pontification?

Deep Dive #1: Cybersecurity Program Governance, Risk Acceptance, and Intra-organization Communication.

We think of a cybersecurity program as a multifaceted, multi-domain activity (almost a living organism) involving organizational dynamics, people, technology, insiders, outsiders, stakeholders….

What have people experienced are the major roadblocks or deal breakers for a healthy cybersecurity program?

CTSC

Deep Dive #1: Cybersecurity Program Governance, Risk Acceptance, and Intra-organization Communication.

Risk acceptance is the process of accepting residual risk (i.e., the risk that remains after controls are applied), and it is a critical part of any risk-based approach to any type of hazard over which we cannot exert full control. In the archetypal case, it involves an *agent* communicating well-grounded risk information to a *principal* who has authority to accept risk on behalf of an organization, or push for greater control. At its best, it is a process of informed decision-making and balancing costs and benefits. In reality, it can be complicated, imperfectly executed, imperfectly understood, entirely ignored…. (our issues with this area was a Finding in 2014).

What experiences do you have with the risk acceptance process? How formal or informal are things in your projects/facilities? Is information security risk acceptance authority distributed, or confined to one role?

What works? What doesn't?

CTSC

Deep Dive #2: Securing Novel Technologies

For our purposes, a “novel technology” is one that is not mature enough and/or not common enough for a robust set of best security practices to have been developed, widely communicated, and iterated on.

Deep Dive #2: Securing Novel Technologies

0. Know what you are securing.
    - Devices, data, people and processes
    - CIA Needs
1. Follow the data
2. Work from the principles that apply to everything:
    - Least Privilege
    - Minimize Attack Surfaces
    - Separation of Concerns
3. Document and monitor so that you can respond and iterate.