ENERGYSEC
SERVING THE INDUSTRY'S SECURITY COMMUNITY SINCE 2004

NIST Cyber Security Framework

Jack Whitsitt
jack@energysec.org | http://twitter.com/sintixerr

(Brief) History/Background

- "Framework to Achieve DHS specified Performance Goals"
- Industry-Driven
- "All Inclusive"
- "Standards" not "Standards"
- Some Vision

Framework Overview

- Three (Main) Components
  - Framework Core
    - Functions, Categories, Subcategories
    - Subcategories = "Outcome oriented **Practices**"
    - "Practices" is my word
  - Framework Implementation Tiers
    - Like Maturity Levels
  - Framework Profile
    - "As-is" and "To-Be" concept from Enterprise Architecture
- http://www.nist.gov/cyberframework/

Framework Core (Structure)

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

Framework Core (Practices)

Function	Category	Subcategory	Informative References
			SR 7.6 • **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1 • **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7
DETECT (DE)	**Anomalies and Events (DE.AE):** Anomalous activity is detected in a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems is established and managed	• **COBIT 5** DSS03.01 • **ISA 62443-2-1:2009** 4.4.3.3 • **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4
		DE.AE-2: Detected events are analyzed to understand attack targets and methods	• **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 • **ISO/IEC 27001:2013** A.16.1.1, A.16.1.4 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4
		DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors	• **ISA 62443-3-3:2013** SR 6.1 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4
		DE.AE-4: Impact of events is determined	• **COBIT 5** APO12.06 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI - 4
		DE.AE-5: Incident alert thresholds are established	• **COBIT 5** APO12.06 • **ISA 62443-2-1:2009** 4.2.3.10 • **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8
	Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events	• **CCS CSC** 14, 16 • **COBIT 5** DSS05.07 • **ISA 62443-3-3:2013** SR 6.2 • **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4
		DE.CM-2: The physical environment is	• **ISA 62443-2-1:2009** 4.3.3.3.8

Framework Implementation Tiers

- Tier 1: Partial
- Tier 2: Risk Informed
- Tier 3: Repeatable
- Tier 4: Adaptive

"The Tier selection process considers an organization's current risk management practices, threat environment, legal and regulatory requirements, business/mission objectives, and organizational constraints."

Profiles

The following steps illustrate how an organization **could** use the Framework to create a new cybersecurity program or improve an existing program.

- Step 1: Prioritize and Scope.
- Step 2: Orient
- Step 3: Create a Current Profile
- Step 4: Conduct a Risk Assessment
- **Step 5: Create a Target Profile**
- Step 6: Determine, Analyze, and Prioritize Gaps
- Step 7: Implement Action Plan

Most Helpful: Core (Practices)

- Practices describe "outcome" security activities
  - Organizations build activities/infrastructure that do a thing described by the Core
- Framework practices in Core:
  - Well-Written
  - Comprehensive
  - Simple Language
  - Linked to more detailed references
- Can be easily used to:
  - Link language across organizations
  - Link frameworks
  - Perform practice gap analysis against requirements

Limits

- Framework Core structure misaligned (incident response)

- Framework suggests four areas of competence
  - Practices (suggestive of controls)
  - Tiers (suggestive of maturity models)
  - Profiles (suggestive of architecture models)
  - "Risk Based" (suggestive of risk management)

- Framework provides **none** of the in-depth knowledge required in the last three areas
  - Users must seek out or develop that competence elsewhere

Even though the framework focuses on Practices and they are clearly written, they still leave organizations with a lot of work to do to become useful

Practices vs. Controls

- Core provides “Practices”, not “Controls”
- Controls maintain system state and should allow testing
- Practices require substantial context to become controls
- Context must help answer:

Who does What When to Achieve which Results to Solve Which Business Problems?

NISTCSF would requires specific knowledge of users’ business environments to answer these questions completely

(even the “what”)

Example NISTCSF “Practice”

DE-AE-4: Detect: Anomalies and Events:

“Impact of Events is Determined”

These words don’t mean anything by themselves and cannot be implemented by themselves

There are no actions or resources assigned to any specific business problem(s)

Un-Answered Practice Questions

- "Impact":
  - What is an impact?
  - To whom is this practice aimed?
  - How is impact expressed?
  - Are there different types of impacts?
  - Can they be compared?
  - Where can impacts occur?
  - Do they cascade? How do they relate?

Un-Answered Practice Questions

- "Event"
  - What is an event?
  - Where can it occur?
  - How is it measured and communicated?
  - By whom to whom?

Un-Answered Practice Questions

- "Determined"
  - Is there a process for this? What is it?
  - How does the process have to scale?
  - Which impacts and events are relevant?
  - To whom and what actions should they be able to take?
  - Using what tools and resources?

Practices vs. Controls

Providing the business and technical context to convert NISTCSF practices into effective and efficient controls solving business problems is where the bulk of the work implementing NISTCSF exists

Tiers, Profiles, and Risk Management programs can help manage this context, but framework users must have that knowledge in-house

Evaluation: Areas of Need

- Strategic Reduction of Risk
- Responsibility Assignment/Clarity
- Risk Management Education/Improvement
- Common Practice Language/Integration
- Coordination/Dialogue Vehicle

Evaluation: Primary Assistance

- ~~Strategic Reduction of Risk~~
- ~~Responsibility Assignment/Clarity~~
- ~~Risk Management Education/Improvement~~
- Common Practice Language/Integration
- Coordination/Dialogue Vehicle

Significant Use Cases

- Framework/Standards linking
- Program Robustness Evaluation
- Cross-Community Communication
- Framework Development
- Controls Comparison/Reduction

Follow-Up

- RFI Issued this year
  - Content addition responses seemed “haphazard” (IMO)
  - Most people happy with NIST retaining stewardship
  - Insufficient resources for using the framework
- New April Workshop in Maryland 4/6 – 4/7
  - Help NIST understand stakeholder awareness and current use of the Framework, the need for an
  - Cybersecurity best practices sharing
  - Future governance of the Framework
- EnergySec Framework classes throughout the year
  - Converting practices to controls
  - Linking business and technology risk
  - Framework design, integration, and use
  - C2M2 & NIST as jumping off points
  - http://events.energysec.org

Summary

- Government led, industry developed
- Not legally mandatory; insurance and peer pressure still factors
- Primarily consists of generic practice statements
- Goal is standardization and integration of language/practices across Stakeholders, not implementation standards
- Does not provide "How" guidance, context, metrics, or process
- Few risk or compliance alignment mechanisms
- Limited utility in existing structure
- But still useful for what it does: **Simplify Practices & Language**
- http://www.nist.gov/cyberframework/

ENERGYSEC
SERVING THE INDUSTRY'S SECURITY COMMUNITY SINCE 2004

Thank You!

Jack Whitsitt
jack@energysec.org | http://twitter.com/sintixerr