A Simplified Approach to Implementing the NIST CSF Within Operational Technologies

Presented to ICS-JWG Fall Conference 2016

Richard Dahl
Founder, CEO
cmplid:// Inc.

cmplid://

the.compliance.daemon

License

Agenda

Who am I

Overview of NIST CSF

Challenges applying the CSF to OT

3 Simplifications

Analysis Process

Richard Dahl

- Founder and CEO of cmplid:// Inc.
- Technology Security Expert with more than 23 years experience
  - First 5 years as Counterintelligence Agent in US Army
  - Extensive technical experience within many industries including
    - Government/Military
    - Bulk Electric
    - Nuclear Power
    - Manufacturing
- Security management methodology zealot
  - Passion for repeatable and consistent processes that produce high quality security programs

Counterintelligence Agent

Sounds like:

Counterintelligence Agent

Sounds like:

Counterintelligence Agent

Looks like:

Counterintelligence Agent

Looks like:

Overview of the NIST CSF

a set of industry standards and best practices to help organizations manage cybersecurity risks

IT IS NOT A SECURITY PROGRAM THAT CAN BE IMPLEMENTED

3 Parts of the Framework

Core Set of cybersecurity activities, desired outcomes, and applicable references that are common across critical infrastructure sectors

Tiers Provide context on how an organization views cybersecurity risk and the processes in place to manage that risk

Profiles Represents the outcomes based on business needs that an organization has selected from the Framework Categories and Subcategories

Risk Based

uses risk management processes to enable organizations to inform and prioritize decisions regarding cybersecurity.

Core Structure

Functions organize basic cybersecurity activities at their highest level.

Categories the subdivisions of a Function into groups of cybersecurity outcomes closely tied to programmatic needs and particular activities.

Subcategories divide a Category into specific outcomes of technical and/or management activities.

Informative References specific sections of standards, guidelines, and practices common among critical infrastructure sectors that illustrate a method to achieve the outcomes associated with each Subcategory.

Core Functions

Identify Develop the organizational understanding to manage cybersecurity risk to systems, assets, data, and capabilities.

Protect Develop and implement the appropriate safeguards to ensure delivery of critical infrastructure services.

Detect Develop and implement the appropriate activities to identify the occurrence of a cybersecurity event.

Respond Develop and implement the appropriate activities to take action regarding a detected cybersecurity event.

Recover Develop and implement the appropriate activities to maintain plans for resilience and to restore any capabilities or services that were impaired due to a cybersecurity event.

Core Structure Excerpt

Function	Category	Subcategory	Informative References
RESPOND (RS)	**Response Planning (RS.RP):** Response processes and procedures are executed and maintained, to ensure timely response to detected cybersecurity events.	**RS.RP-1:** Response plan is executed during or after an event	• **COBIT 5** BAI01.10 • **CCS CSC** 18 • **ISA 62443-2-1:2009** 4.3.4.5.1 • **ISO/IEC 27001:2013** A.16.1.5 • **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8
	Communications (RS.CO): Response activities are coordinated with internal and external stakeholders, as appropriate, to include external support from law enforcement agencies.	**RS.CO-1:** Personnel know their roles and order of operations when a response is needed	• **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • **ISO/IEC 27001:2013** A.6.1.1, A.16.1.1 • **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8
		RS.CO-2: Events are reported consistent with established criteria	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 • **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8
		RS.CO-3: Information is shared consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.2 • **ISO/IEC 27001:2013** A.16.1.2 • **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4
		RS.CO-4: Coordination with stakeholders occurs consistent with response plans	• **ISA 62443-2-1:2009** 4.3.4.5.5 • **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8
		RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness	• **NIST SP 800-53 Rev. 4** PM-15, SI-5
	Analysis (RS.AN): Analysis is conducted to ensure adequate response and support recovery activities.	**RS.AN-1:** Notifications from detection systems are investigated	• **COBIT 5** DSS02.07 • **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 6.1 • **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 • **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-

Tiers

provide context on how an organization views cybersecurity risk and the processes in place to manage that risk

Framework Tiers

Tiers do not represent maturity levels

Framework Profiles

the alignment of the Functions, Categories, and Subcategories with the business requirements, risk tolerance, and resources of the organization

Framework Profiles

Framework Profiles can be used to describe the current state or the desired target state of specific cybersecurity activities

Current Profile indicates the cybersecurity outcomes that are currently being achieved

Target Profile indicates the outcomes needed to achieve the desired cybersecurity risk management goals

Given the complexity of many organizations, they may choose to have multiple profiles, aligned with particular components and recognizing their individual needs.

What is the NIST Framework?

Core view of risk

Tiers view of program maturity

Profiles view of security posture

Implementation Steps

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

1. Prioritize and Scope

Identify business processes and system functions that require protection

2. Orient

Identify resources supporting those business processes or system functions, regulatory requirements, risk approach and associated threats and vulnerabilities thereto

3. Create a Current Profile

The organization develops a Current Profile by indicating which Category and Subcategory outcomes from the Framework Core are currently being achieved

4. Conduct a Risk Assessment

This assessment could be guided by the organization's overall risk management process or previous risk assessment activities

5. Create a Target Profile

The organization creates a Target Profile that focuses on the assessment of the Framework Categories and Subcategories describing the organization's desired cybersecurity outcomes

6. Determine, Analyze, and Prioritize Gaps

The organization compares the Current Profile and the Target Profile to determine gaps

7. Implement Action Plan

The organization determines which actions to take in regards to the gaps, if any, identified in the previous step

Challenges Applying the CSF to O/T

NIST and many other security control libraries are Information-centric

The variety of O/T equipment is significant, from simple transmitters to full fledged computers

Personnel generally have less experience with technology security than IT environments

Profiles, as defined, are unwieldy

3 Simplifications

Resource-Based

The standards apply to various resource types

Attribute-Informed

The standards are implemented based on characteristics (attributes) of the resources

Objective-Driven

The standards are designed to realize specific security objectives

Simplification #1

Resource-Based

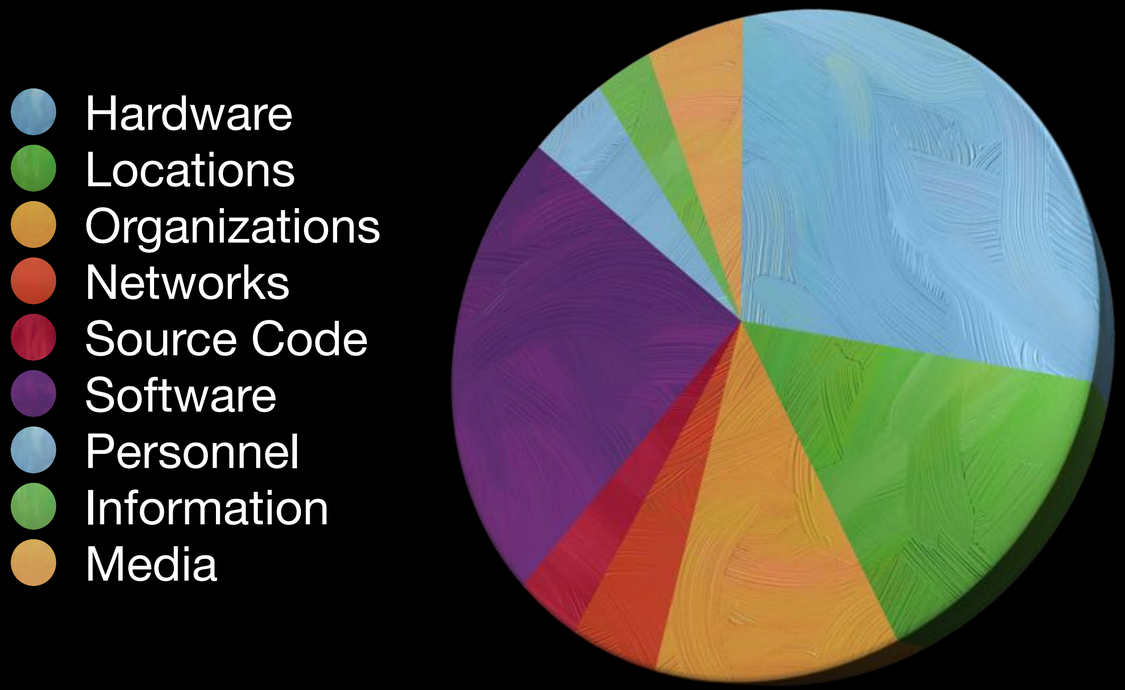
Resource Based

Confusing application

“Cyber Security” sounds like a technical issue, but...

Control Applicability

Security is a business issue, not an IT/OT issue!



Example of Resource Applicability

Training and Background Investigations apply to Personnel

Policies and Procedures generally apply to Organizations

Firewalls and IDS apply to Networks

Physical Security mechanisms apply to Locations

Information Labeling applies to Information and Media

Authenticating Users applies to Hardware and Software

User Input Validation applies to Source Code

Inheritance

The relevant security mechanisms from one resource are generally inherited by other resource types

Simplification #2

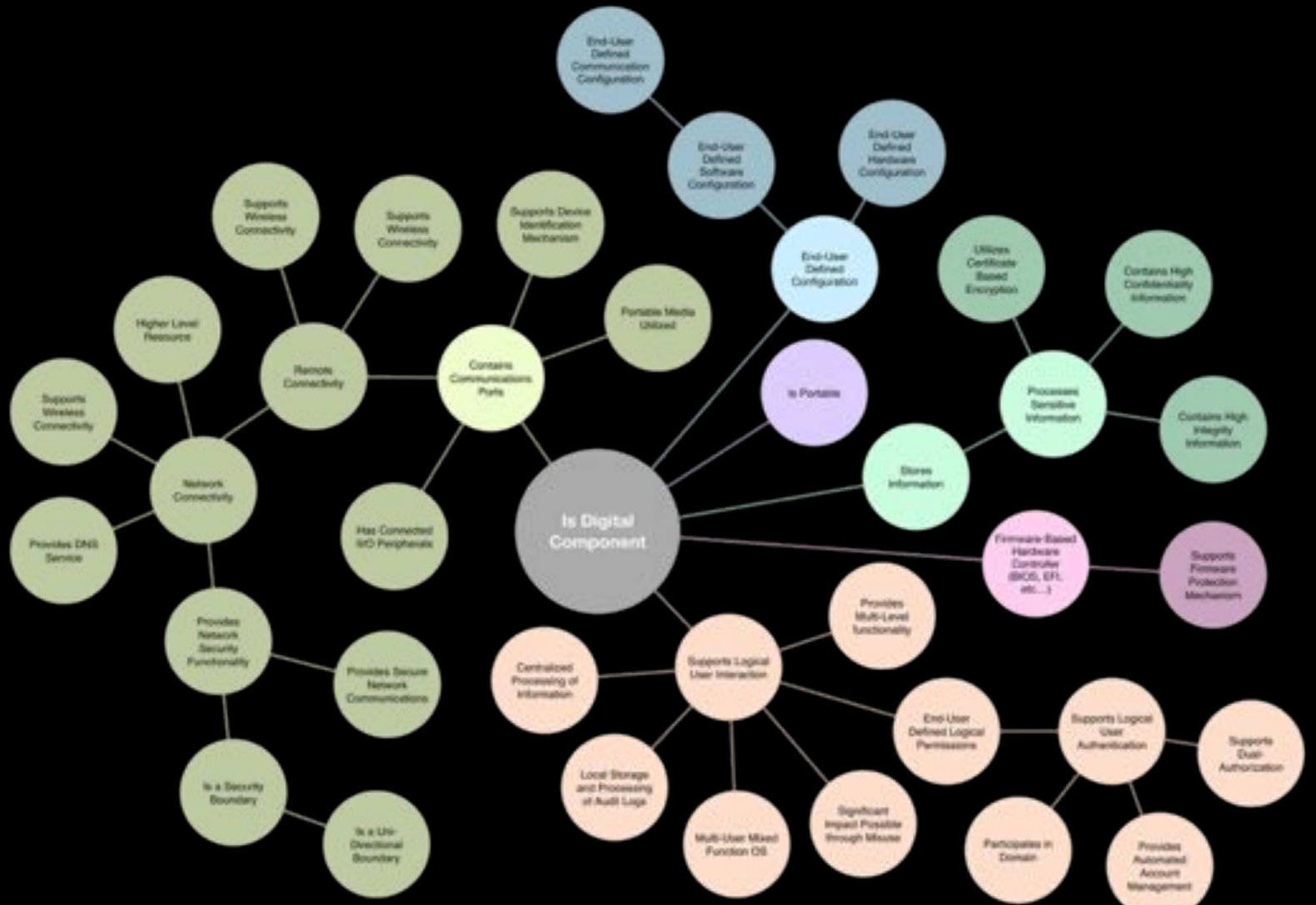
Attribute-Informed

Attributes

Any characteristic of an organizational Resource that:

- Indicates inclusion in a security program
- Indicates a security standard is necessary to protect a Resource
- Indicates how a security standard will be implemented for a Resource

Attribute Hierarchy



cmplid://

Attribute Result

Associate the security controls and detailed security knowledge with relevant, familiar, and understandable characteristics of organizational Resources

Consistent Interpretation

Attributes enable consistent interpretation of security Standards

The interpretation of the Standards is what always happens... it is just not usually documented (very well)

Everyone who looks at the cyber security Standards interprets their meaning based on their own understanding of security and their level of technical competence

The real issue is whether the individual interpretations are consistent with one another throughout the enterprise

Simplification #3

Objective-Driven

Security Objectives

foundation for all risk analysis

purpose of the security Standards

consequence of failure or absence of the Standards

Security Objectives

Consistent with the NIST CSF Functions

ID.AM-2: Software platforms and applications within the organization are inventoried

ID.RA-3: Threats, both internal and external, are identified and documented

PR.IP-3: Configuration change control processes are in place

PR.AC-2: Physical access to assets is managed and protected

PR.AT-2: Privileged users understand roles & responsibilities

Security Objectives

PR.IP-1: A baseline configuration of information technology/ industrial control systems is created and maintained

PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy

DE.CM-5: Unauthorized mobile code is detected

RS.CO-1: Personnel know their roles and order of operations when a response is needed

Analysis Process

Resource Types: identify applicable Standards

↳ **Compliance Scopes:** associate Standards to Resources

↳ **Standard Maps:** group related Standards

↳ **Control Maps:** end-user implementation mechanisms

Compliance Scopes

Resource Type specific NIST CSF Profiles

Relevant security Standards applicable to a specific Resource Type based on defined Resources Characteristics

NIST SP 800-53 Examples

- High Baseline Location
- Moderate Baseline Software
- Low Baseline Source Code

Standard Maps

Group of Standards within a Compliance Scope that:

- Share common Security Objectives
- Share common implementation mechanism (Controls)

Therefore they will share common determining characteristics (Attributes)

Control Maps

Group one or more organizationally defined implementation mechanisms (Controls) that:

Fulfill the Standards for a Standard Map

Implement the Standards either:

Directly, Alternately, or through Inheritance

Summary

The NIST CSF provides 3 distinct ways of looking at your security program: risk, maturity, security posture

Comprehensive profiles are unwieldy

Application of the NIST CSF for O/T environments can be simplified through consistent application of a resource-based, attribute-informed, objective-driven security management methodology

Thank You

Questions?

Comments.

Concerns!