Tactical “SCM/ESA” View for Cyber Security Framework (CSF)

Collaboration with

Mike Davis
SPAWAR SoS/MA Engineer (Ret.) / Cyber Security Consultant

and

Rick Smith
Cyber Clarity

Mike.Davis.SD@gmail.com
And
rick@cyberclarity.com
What’s Wrong With This Security?

What level of protection is really provided here?

The gates were fully locked, properly configured and validated. I could not get through them. But.... Thus Cyber can be an illusion...

When a capability is “invisible”, like IA, safety, reliability, etc, what you see is not the whole picture!
Notional Roadmap to CSF Execution

“CSF” execution & value points.

Threat overview / perspective

CSF background / pressure points

Tactical view

Summary

Be wary of a false sense of security
Monitor & measure your security environment
using a SCM / SIEM like tool!
Cyber Security – Overall Status
(Senior IA VIP (Mike Jacobs) - *same issues as 40-50 years ago*, but better in last 10)

<table>
<thead>
<tr>
<th>Category</th>
<th>Status</th>
<th>Trending</th>
</tr>
</thead>
<tbody>
<tr>
<td>Technology</td>
<td>(\text{---})</td>
<td>(\text{G}) We have what we NEED NOW</td>
</tr>
<tr>
<td>Business</td>
<td>(\text{---})</td>
<td>(\text{Y}) Some LSIs resist change</td>
</tr>
<tr>
<td>Policy</td>
<td>(\text{---})</td>
<td>(\text{Y}) Legislation poor Can’t be voluntary</td>
</tr>
<tr>
<td>Procedures / standards</td>
<td>(\text{---})</td>
<td>(\text{G}) NIST done well Need uniform implementation</td>
</tr>
<tr>
<td>Education</td>
<td>(\text{---})</td>
<td>(\text{G}) NICE, 170+ CAEs (schools) 10,000+ / year</td>
</tr>
<tr>
<td>Leadership</td>
<td>(\text{---})</td>
<td>(\text{R}) Complexity vs CISO C-suite complacency and ability to absorb</td>
</tr>
<tr>
<td>Awareness</td>
<td>(\text{---})</td>
<td>(\text{G}) Education starting earlier, STEM, NICE</td>
</tr>
</tbody>
</table>

*We all need to provide an integrated, cyber package that is affordable*
Gartner's 2013 Hype Cycle for Emerging Technologies

- How do we prove end-2-end security?
- Everything connected to everything? Comms Secure?
- Automation = machines in control? M2M Secure?
- Pervasive new technologies? Built secure?
- CYBER is all about SECURE: technologies, DATA and communications!

"ALL" the technologies need built in security ... AND... support data security / Privacy!
SO... what does matter in Cyber?

CYBER is fundamentally all about **TRUST** and **DATA**
(Identity / authentication / secure comms -- provenance, quality, pedigree, assured)

It’s NOT about expensive new cyber capabilities / “toys”
but more about the **interoperability “glue”** (distributed trust, resiliency, automation, profiles)

90+% of security incidents are from **lack of doing the basics**!
HAVE effective **Security Continuous Monitoring (SCM / SIEM)** – a MUST DO!
USE enforced: cyber hygiene, enterprise access control, & reduce complexity (APLs)
*Shift from only protecting the network, to the **DATA security itself** – information centric view*

Embrace your **Risk Management Plan (RMP)** – **LIVE IT**!
Have an enforceable **security policy** – what is allowed / not – train to it
*KNOW your baseline* - Protect the business from the unknown risks as well
Employ a **due diligence level of security** – then **transfer residual risks**!

You can **NOT buy cyber**, so **manage the cyber BASICS well**!
An achievable 90-95% solution to MOST vulnerabilities – **stabilize the environment**!
Yes, It is ALL about the **DATA**!

**2020 Vision**

(Courtesy of Dan Green / SPAWAR):

*Themes* and Memes (Technology vs Technology Adoption)

*Convergence* = Genomics, Robotics, Informatics, Nanotech (each a $B+$ market)

"**CBAD**" = Cloud, Big Data, Analytics, Data Science (are you ‘all-in?’)

*Telematics* = Sensing robotics, Cyber Physical Systems (will kids need to learn to drive?)

*Interactive 3D* = Augmented Reality, HTML 5, Three.js (3D graphics for WebGL)

*Embedded Computing* = eHPC, Tessel (mCPU / Java), Programmable hardware

*LBS* = Location Based Services, IPS, Beaconing, NFC

*IoT* = Internet of Things, M2M, Quantified Self

*Mobilization* = Preparation for Conflict/Competition, Autonomy, The Draft

*STEM* = Science Technology Engineering Math, Generation NOW, Old Dogs (YOU)

In a data-centric world, we need **Privacy by Design (PbD)**

*Meme*: an idea, behavior, or style that spreads from person to person within a culture

10 year series, 63,437 incidents, 1367 breaches, 95 countries

WHAT
- 92% incidents described by just nine patterns
- from geopolitical attacks to large-scale attacks on payment card system

Sectors
- Public (47, 479), Information (1132) and Finance (856)

Threats (%)
- POS intrusions - 31
- Web App Attacks - 21
- Cyber espionage - 15
- Card Skimmers - 14
- Insider misuse - 8
- Crimeware - 4

Mitigations
- restrict remote access
- enforce password policies
- Minimize “non” POS activity on those terminals
- Deploy A/V (everywhere, POS too)
- evaluate threats to prioritize treatments
- Look for suspicious network activity
- Use two-factor authentication

We have met the cyber enemy, and they are US

HYGIENE Factors

See also - Ponemon Institute’s cyber report
Key threats – from cost based activities
Malware, malicious insiders and web-based attacks
Integrated Business RMP Approach
+ Especially for Small / Medium Business (SMB) = THE ANSWER +

Company Vision
(business success factors)

Security Policy
(mobile, social media, etc)

C&A / V&V
(effective / automated)

Known Baseline
(security architecture)

Insider Threat
Company Intel
(open source, FB, etc)

CMMI / Sustainment
(SoPs / processes)

SCM / SIEM
(monitor / track / mitigate)

Privacy by Design
(manage PII, HIPAA, compliance)

MSS / vCISO
(3rd party IV&V support)

Data Centric Security
(DLP, reputation based methods)

Cyber insurance
(broker & legal council)

Education / Training
(targeted, JIT, needs based)

Common Risk Management Plan (RMP) model
AND IAW the NIST Cybersecurity Framework
DoD Cyber S&T Roadmap

What matters? Key Capability Gaps / Areas “4+1”

Assuring Effective Missions
- Assess and control the cyber situation in mission context
  - Support essential business success functions

Agile Operations
- Dynamically reshape cyber systems as conditions/goals change, to escape harm
  - Autonomous responses and C3 Tools

Resilient Infrastructure
- Withstand cyber attacks, and sustain or recover critical functions
  - Environment is robust and self-healing

Trust
- Establish known degree of assurance that devices, networks, and cyber-dependent functions perform as expected, despite attack or error
  - Mixed trust levels in heterogeneous space

Gaps are not “things / capabilities” but integration and interoperability!
Overview of Framework

• Framework Core
  – Core presents industry standards, guidelines, and practices
  – Focus on 5 functions (Identify, Protect, Detect, Respond, Recover)
  – Start by using the CSF function you need most – then expand out

• Framework Implementation Tiers
  – Provide a way to view cybersecurity risk and to manage the risk
  – Consideration from current risk management practices, threat environment, legal and regulatory environment, mission and organizational constraints
  – Organization sets thresholds of tiers – best done by sector (i.e., use “ISAC”)

• Framework Profile
  – Organization selecting the Framework Category and Subcategory
  – Looking to quantify “As Is” and “To Be” (Target Profile by sector)
  – Used to conduct self-assessment and communications within an organization AND also a third party independent assessment = baseline!
Framework Roadmap
what’s still needed to enhance CSF

Automated Indicator sharing – more effective ways to detect and respond to events

Conformity Assessment – capability meets requirements within CSF

Cybersecurity workforce – adapt, design, develop maintain and improve security practices.

Data Analytics – tools with new computing methods = new processes to analyze all data

Agency alignment – Integrate CSF & RMF to enhance policy, reduce burden with common postures

International alignment – help effective operate globally and manage new risks.

Technical privacy standards – translate FIPPs into methods for effective privacy metrics / risks.

Tools to easily assess and organization’s CSF posture, Support analytics / trending, broad use – including privacy
One notional Tactical View that focuses On ID, detect & respond:

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

Understand, Validate, Execute, Sustain

• Building a Positive Security Posture for an organization requires a focused approach
• Building a Compliance Automation Reporting (CAR) process is your first step
• Once an organization is reached a State of Positive Health, Enhanced Situational Awareness (ESA) can be executed
• Sustainability of ESA is crucial to a Positive Security Posture
• Integrates easily in a Compliance Risk Scoring Approach
• Meets CyberScope intentions
The BIG PICTURE

Prepare for a Positive State of Health

Executing ESA

Sustaining State of Health with People, Process and Technology
POA&M Workflow

- **Maintain Current knowledge of vulnerabilities**
  - National Vulnerability Database

- **Compare NVD with found vulnerabilities and prioritize**
  - Scanned Data

- **Map vulnerabilities to FISMA controls**
  - FISMA Controls

- **Maintain Situational Awareness on your POA&M**
  - POA&M Reports

**Manage FISMA**

**Vulnerability Management Process**

**POA&M Process**

- **Maintain Current knowledge of vulnerabilities**
  - National Vulnerability Database

- **Compare NVD with found vulnerabilities and prioritize**
  - Scanned Data

- **Map vulnerabilities to FISMA controls**
  - FISMA Controls

- **Maintain Situational Awareness on your POA&M**
  - POA&M Reports

**Manage FISMA**

**Vulnerability Management Process**

**POA&M Process**

- **Maintain Current knowledge of vulnerabilities**
  - National Vulnerability Database

- **Compare NVD with found vulnerabilities and prioritize**
  - Scanned Data

- **Map vulnerabilities to FISMA controls**
  - FISMA Controls

- **Maintain Situational Awareness on your POA&M**
  - POA&M Reports

**Manage FISMA**

**Vulnerability Management Process**

**POA&M Process**

- **Maintain Current knowledge of vulnerabilities**
  - National Vulnerability Database

- **Compare NVD with found vulnerabilities and prioritize**
  - Scanned Data

- **Map vulnerabilities to FISMA controls**
  - FISMA Controls

- **Maintain Situational Awareness on your POA&M**
  - POA&M Reports

**Manage FISMA**
Architectural View of ESA with CAR

**Compliance Automation Report**
Employs GOTS & open source software
- Reduced cost of ownership
- Vendor Agnostic
- Conforms to Federal standards
- Real-time, federated architecture
- Consumes and Produces SCAP (XCCDF)
CAR Dashboard and Application
(Advantages of using CAR methods)

• CAR’s Functions
  – Provides a unified dashboard to access and display multi-vendor security compliance and risk applications at the organizational level (lowest level)
  – Inputs FDCC scores in XCCDF format
  – Groups FDCC fail scores into 7 risk categories (0-6, risk category 0 = 100% compliance)
  – Provides a per desktop compliance score (0-100%) vs. risk score (0 – 7) of the organization on a two-dimensional graph that clearly identifies outliers
  – Transforms XCCDF to an industry standard lightweight data interchange format and compresses it to **two orders of magnitude** less than original format
  – Distributes the compressed risk and compliance data up the organizational hierarchy via the Federated Framework

Agencies can gain the ability to easily share and distribute compliance and risk information with CAR to provide a global defensive posture of your networks
Integrating this into a large enterprise

Data Sharing to HQ to provide Situational Awareness (SA)

Subordinate Organization 1

Subordinate Organization 2
Data Flow Chart for a Federated Framework at each Tier 3 level

- Malware Detection
- Compliance Server
- DB Security
- Network Correlator
- SQL or BIG DATA Architecture/Storage (Partnering with TeraData)
- Cyber Analytics (API/Web Service)
  - Outlier Threshold Setting
  - Threat Analysis
  - Threat Vectoring
  - Building blocks for Predictive Analytics

Risk Management
Data Model of what you can view

Site

Site Detail

Location / Description
POC
POC Contact Info
Roles of POC
Assets Owned by POC
IP/Subnet
POA&M to the asset
Last Vulnerability Scan

Other Assets connected on the subnet

Other Assets connected on the subnet

Other Assets connected on the subnet

Other Assets connected on the subnet

Assets Owned by POC
• IP/Subnet
• POA&M to the asset
• Last Vulnerability Scan

Other Data tied to the asset

System Logs

CMDB

Network Logs

Compliance

Security Logs

Other Data

Data Model of what you can view

System Logs

CMDB

Network Logs

Compliance

Security Logs

Other Data

21
Building a common Taxonomy

• 1) Describe their current cybersecurity posture;
• 2) Describe their target state for cybersecurity;
• 3) Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
• 4) Assess progress toward the target state;
• 5) Communicate among internal and external stakeholders about cybersecurity risk.
Describe the current cybersecurity posture;

• Setting up company approved baseline metrics
• Use the CSF’s “as-is” profile to baseline security environment – that should map to organization’s RMP, with current business needs
• Example (Outlier Reports)
Outlier Explanation

Unacceptable range of compliance (Outlier)

10% out of compliance

In compliance

Thresholds between circles critical to map to business AND protection needs

Identify, track and mitigate the critical outliers first (= POA&M).
Example outlier
Old way of viewing a *FDDC report*

Old Approach

No way of knowing the severity / criticality of boxes that pass (e.g., red 100).
Applying *Severity Rating* to the FDCC Report

**Two inputs** – Severity and Metric

NOW – the key high severity problems are identified regardless of metric level.
Outlier Reports 1 of 3

You set the thresholds
Can do multiple views
And prioritize mitigations

Create multiple Outlier Reports

Notional to Reality
Outlier Reports 2 of 3

Create a Framework that inputs Severity & a Metric
• Idea is to create ways to measure impact universally
• Allows each client to set their OWN impact
• Still aligns with Strategic Data Strategy with some proprietary approach

Create Multiple Outlier reports that help show Impact to the Mission
• Common Operational Picture
• Intuitive
• Can be re-purposed
Outlier Reports 3 of 3
Defining Severity & Metric in other areas

Severity - Measuring against known vulnerabilities with a level of impact
• Cat1, Cat2, Cat 3 Finding
• Patches
• Signatures
• Malwares

Metric – Component that shows average usage for sustainment
• Time
• Software Version
• Certain Percentage score

<table>
<thead>
<tr>
<th>Item</th>
<th>Severity</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>FDCC</td>
<td>Registry items</td>
<td>FDCC Score (0 – 100)</td>
</tr>
<tr>
<td>Network Operations</td>
<td>Bandwidth Usage</td>
<td>Time of the day</td>
</tr>
<tr>
<td>Configuration Management</td>
<td>Software Vulnerability</td>
<td>Versions</td>
</tr>
</tbody>
</table>
Aggregate View of FDCC/USCGB Report in our pilot application

<table>
<thead>
<tr>
<th>LOCATION</th>
<th>PROFILE</th>
<th>#</th>
<th>L%</th>
<th>M%</th>
<th>H%</th>
</tr>
</thead>
<tbody>
<tr>
<td>BALTIMORE</td>
<td></td>
<td>29</td>
<td>70%</td>
<td>24%</td>
<td>6%</td>
</tr>
<tr>
<td>WASHINGTON DC</td>
<td></td>
<td>48</td>
<td>71%</td>
<td>27%</td>
<td>2%</td>
</tr>
<tr>
<td>DENVER</td>
<td></td>
<td>40</td>
<td>73%</td>
<td>17%</td>
<td>10%</td>
</tr>
<tr>
<td>ALBUQUERQUE</td>
<td></td>
<td>31</td>
<td>75%</td>
<td>16%</td>
<td>9%</td>
</tr>
<tr>
<td>HOUSTON</td>
<td></td>
<td>32</td>
<td>76%</td>
<td>21%</td>
<td>3%</td>
</tr>
<tr>
<td>PRINCETON</td>
<td></td>
<td>46</td>
<td>79%</td>
<td>15%</td>
<td>6%</td>
</tr>
<tr>
<td>CLEVELAND</td>
<td></td>
<td>23</td>
<td>79%</td>
<td>13%</td>
<td>8%</td>
</tr>
<tr>
<td>MIAMI</td>
<td></td>
<td>42</td>
<td>79%</td>
<td>14%</td>
<td>7%</td>
</tr>
</tbody>
</table>
Outlier Report on one section in our pilot application

**FINANCE SERVICES: FDCC SCORING VS. SEVERITY**

<table>
<thead>
<tr>
<th>SEVERITY</th>
<th>FDCC SCORING</th>
<th>#</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>40</td>
</tr>
<tr>
<td></td>
<td></td>
<td>104</td>
</tr>
<tr>
<td></td>
<td></td>
<td>571</td>
</tr>
<tr>
<td>50%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>75%</td>
<td></td>
<td></td>
</tr>
<tr>
<td>100%</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Describe their target state for cybersecurity;

• Understanding the targeted area and what level we need to set them is implemented through **Threshold Settings**.

• Leverage the “target profiles” in the CSF for your sector – seek out a representative “ISAC” to follow common thresholds / key metrics

EG: Multi-State Information Sharing and Analysis Center (ISAC)
http://msisac.cisecurity.org/
Outliers will help to set up the baseline status of Health and will be used to set up thresholds.

Algorithm
Risk Score = Total Assets/number of severity
Threshold Settings 2 of 3

Setting up a threshold against the **Highs** will alert us when each location is exceeding the allowable threshold.

### FDCC PLATFORM SECURITY POSTURE

<table>
<thead>
<tr>
<th>LOCATION</th>
<th>PROFILE</th>
<th>#</th>
<th>L%</th>
<th>M%</th>
<th>H%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Think Pro Model MB766xx/A</td>
<td></td>
<td>28</td>
<td>40%</td>
<td>25%</td>
<td>35%</td>
</tr>
<tr>
<td>Dell Dimension C521</td>
<td></td>
<td>20</td>
<td>40%</td>
<td>40%</td>
<td>20%</td>
</tr>
<tr>
<td>Dell Dimension 8100</td>
<td></td>
<td>20</td>
<td>40%</td>
<td>25%</td>
<td>35%</td>
</tr>
<tr>
<td>Dell Dimension 9200c</td>
<td></td>
<td>20</td>
<td>45%</td>
<td>35%</td>
<td>20%</td>
</tr>
<tr>
<td>Think Pro Model MB166xx/A</td>
<td></td>
<td>28</td>
<td>47%</td>
<td>32%</td>
<td>21%</td>
</tr>
<tr>
<td>Cisco Router 7500</td>
<td></td>
<td>21</td>
<td>48%</td>
<td>38%</td>
<td>14%</td>
</tr>
<tr>
<td>Dell Dimension 5150</td>
<td></td>
<td>20</td>
<td>50%</td>
<td>30%</td>
<td>20%</td>
</tr>
<tr>
<td>Think Fire X4150 Server SW 2.0</td>
<td></td>
<td>8</td>
<td>51%</td>
<td>12%</td>
<td>37%</td>
</tr>
</tbody>
</table>

**Note:** The highlighted numbers indicate the threshold scores for each location.
Threshold Settings 3 of 3

<table>
<thead>
<tr>
<th>Location</th>
<th>Asset Over Threshold over 10%</th>
<th>Cat Findings causing the issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>Virginia</td>
<td>192.168.1.23</td>
<td>CVE 204-5098</td>
</tr>
<tr>
<td></td>
<td>192.215.1.23</td>
<td>CVE 34-6098</td>
</tr>
<tr>
<td>Michigan</td>
<td>168.2.3.5</td>
<td>CVE 120-7864</td>
</tr>
<tr>
<td></td>
<td>168.4.3.5</td>
<td>CVE 204-5098</td>
</tr>
<tr>
<td>New York</td>
<td>172.3.5.78</td>
<td>CVE 204-5098</td>
</tr>
<tr>
<td></td>
<td>172.3.5.78</td>
<td>CVE 120-7864</td>
</tr>
</tbody>
</table>

Using the NVD CVE as a relative measure and then use known mitigations!

http://nvd.nist.gov/
Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;

• Understanding the basic reporting and adding indicators to help prioritize the content
  – I.E (FDCC/USCGB graphs)

• Plan for the key mitigations – “RoI” – POA&M
Continuous Monitoring to help identify and prioritize outliers and threshold settings.
Assess progress toward the target state

• Defining baseline metrics through Outlier Reports and Threshold Settings can help your organization Assess Progress.

• Once you have set up the basic metrics, your organization can move into Threat Vectoring and Active Threat Management.
Assess progress toward the target state (cont)

<table>
<thead>
<tr>
<th>Data Sources</th>
<th>Algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td>Known Alerts</td>
<td>Outlier</td>
</tr>
<tr>
<td>Threshold Setting</td>
<td></td>
</tr>
<tr>
<td>Known Behavior</td>
<td>Threat Vectoring</td>
</tr>
<tr>
<td>Outside Data Source</td>
<td></td>
</tr>
<tr>
<td>Not waiting for trouble, Seek trouble</td>
<td>Active Threat Management</td>
</tr>
</tbody>
</table>

Gather Intelligence

Explore the internet
Communicate among internal and external stakeholders about cybersecurity risk.

• *Building a Common Operation Picture (COP)* and sharing definitions can help improve communications with stakeholders

• Having an open architecture to help communicate with other disparate data sources

• Implementing SCAP to provide automated reporting to other stakeholders
Open Architecture
Data Flow Chart for a Federated Framework at each Tier 3 level

Cyber Analytic Processes

Data Storage

Outliers
Thresholds
Threat Vectoring
Threat Analysis

Web Services
- Exposed API
- Documented Data Structures

Message Management Services

Enterprise Service Bus

Malware Detection
Compliance Server

Risk Management

DB Security
Network Correlator
IDS

Data Flow Chart for a Federated Framework at each Tier 3 level
### Sample system interactions

<table>
<thead>
<tr>
<th>System1</th>
<th>Sub System1</th>
<th>A-System</th>
<th>Final Approval</th>
</tr>
</thead>
<tbody>
<tr>
<td>15 Controls – Medium</td>
<td>10 Controls - Medium</td>
<td>18 Controls</td>
<td>12 Controls</td>
</tr>
<tr>
<td>AC-1, 2,5</td>
<td>AC-1,3,4 (2 Cat?,5)</td>
<td>AC 1,3,4,5,7,9</td>
<td>AC 1,5 Waiver 2, 3,4</td>
</tr>
<tr>
<td>Vulnerability</td>
<td></td>
<td></td>
<td>ATO</td>
</tr>
</tbody>
</table>
Data flow through the open architecture

Data Sources

- System Logs
- CMDB
- Network Logs
- Compliance
- Security Logs
- Other Data

API Calls to the Data Sources

- API/ Web Service for System Log
- API/ Web Service for Network Log
- API/ Web Service for Security Log
- API/ Web Service for Compliance Info

Enterprise Service Bus

Big Data Storage

Create a Common Operation Picture (COP)
Share Views
Common
Operational Picture

DHS/NPPD

Organization A

Organization B
Applying SCAP to help automate communications
Common Operation Picture for CAR

- A vendor neutral network security capability
- Aggregates and distributes the networks’ defensive posture across the organizational hierarchy
- SCAP compliant
Applying an interface to the data model

- Reduce Triage Response Time
- Full Situational Awareness (SA)
- Asset Awareness
- POCs and Location

One Asset View

Location

Cyber SA View

POC

Compliance (POA&M)
After sustaining an organization, move into **Active Threat Management (ATM)**
1. Digital DNA detects zero-day malware on a host
2. Agent framework distributes malware signature to CATD
3. CATD monitors network for new malware signature, correlates signature, and runs business logic against data
4. CATD sends required network changes to block the spread of the malware from infected host to ATM
5. The ATM sends TTP the appropriate information to open ticket and alert security/network personnel
6. Human then accepts or denies suggested remediation
7. TTP communicates back to ATM server with response
8. ATM signals DDN to configure network devices to protect network from new malware if applicable
9. ATM distributes malware signature to all sites in federation and sends confirmation of applied network change to CATD if applicable
10. CATD sends confirmation of change back to ATM server if applicable and updates Black/White list
11. ATM sends confirmation of change back to TTP for ticket closure if applicable or apply open issues to RM
Apply ATM to all Assets

Correlate ATM Findings across the Enterprise

Correlate Vulnerability Scans and other Intel across the environment

Botnet_File.Exe
Other Assets connected to that subnet

ZeroDay_File.Exe
Other Assets connected to that subnet

Botnet_File.Exe
Other Assets connected to that subnet

ZeroDay_File.Exe
Other Assets connected to that subnet

Same Vulnerability Files found across GEO Locations
**Business & Cyber Security opportunities**
(Overall KEY functions & related System Engineering / Integration efforts)

**IT / Cyber Global factors – user pull**

<table>
<thead>
<tr>
<th>World-wide B2B</th>
<th>IoT / M2M</th>
<th>Consumerization of IT</th>
<th>Privacy / Data</th>
</tr>
</thead>
<tbody>
<tr>
<td>Trust / cloud / sharing</td>
<td>Automation / Sensors</td>
<td>Phones / wireless / <strong>apps</strong></td>
<td>IP / PII / compliance</td>
</tr>
</tbody>
</table>

**GAPS / Needs**
(from the Federal cyber priority council S&T gaps)

<table>
<thead>
<tr>
<th>TRUST</th>
<th>Resiliency</th>
<th>Agile operations</th>
<th>Effective missions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributed / MLS</td>
<td>SW / apps / <strong>APIs</strong> / services</td>
<td>BE the vanguard / integration</td>
<td>Business success factors</td>
</tr>
</tbody>
</table>

**Vulnerabilities / Threats**
(Verizon BDR, Forbes, etc threat reports - what ails us most)

<table>
<thead>
<tr>
<th>CM / Hygiene</th>
<th>Access control</th>
<th>TOP security mitigations</th>
<th>Risk Mgmt</th>
</tr>
</thead>
<tbody>
<tr>
<td>patching / <strong>settings</strong></td>
<td>Authentication is key</td>
<td><strong>Whitelist</strong>, patch, limit access</td>
<td>Adhoc / not global</td>
</tr>
</tbody>
</table>

**Future Opportunities**

*Effective Business risk management (BRM) = cybersecurity framework (CMMI / RMF / COBIT)*

Reducing business risk / liabilities...
Managed security services (MSS) & cyber insurance...

<table>
<thead>
<tr>
<th>SIEM / SCM</th>
<th>Mobile Security</th>
<th>Mitigate Obsolescence</th>
<th>Data Security</th>
</tr>
</thead>
<tbody>
<tr>
<td>QA hygiene / sensors</td>
<td>Poor apps / IOS weak billions users = volume</td>
<td>Minimize patching, legacy vulnerabilities OA / modularity / <strong>APIs</strong> &amp; SCRM</td>
<td>Predictive analytics</td>
</tr>
</tbody>
</table>

“**CAR / ESA”** / simple tools! **Privacy by design**
Summary

• Applying algorithms to help define metrics
• Aggregate the metrics to define Threshold Settings – *use & map to the CSF tiers!*
• Once your baseline metrics have been defined, Threat Vectoring can be achieved
• Moving to proactive posture through Active Threat Management
• **Harmonize your environment to CSF functions** – *And soon* – especially if you do ANY federal work = FAR!

Mike.Davis.SD@gmail.com
And
rick@cyberclarity.com
Improve Time and Resource on POA&M Process

NOW - 3 – 6 months

After - ½ the time
How to reduce Time and Resources - 1 of 5

1st Step

NIST 800-53 Rev 4 PDF Version

AC-11 SESSION LOCK

Control The information system:

a. Prevents further access to the system by initiating a session lock after [Assignment: organization-defined time period] of inactivity or upon receiving a request from a user; and

b. Retains the session lock until the user reestablishes access using established identification and authentication procedures.

Supplemental Guidance: Session locks are temporary actions taken when users stop work and move away from the immediate vicinity of information systems but do not want to log out because of the temporary nature of their absences. Session locks are implemented where session activities can be determined. This is typically at the operating system level, but can also be at the application level. Session locks are not an acceptable substitute for logging out of information systems, for example, if organizations require users to log out at the end of workdays. Related control: AC-7.

Control Enhancements:

(1) SESSION LOCK | PATTERN HIDDING DISPLAYS

The information system conceals, via the session lock, information previously visible on the display with a publicly viewable image.

Supplemental Guidance: Publicly viewable images can include static or dynamic images, for example, patterns used with screen savers, photographic images, solid colors, clock, battery life indicator, or a blank screen, with the additional caveat that none of the images convey sensitive information.
How to reduce Time and Resources - 2 of 5

2nd Step

Scanned Data → FISMA Controls

Management Process

Nessus Scan in an XML Format

IA Controls in an XML Format
How to reduce Time and Resources - 3 of 5

3rd Step

Key word searches formatted into XML

Key Word Session

<keyword word="SESSION">AC-10 AC-11 AC-11(1) AC-12 AU-14 AU-14(1) AU-14(2) AU-14(3) IA-11 MA-4 MA-4(5) SC-10 SC-15(1) SC-23 SC-23(1) SC-23(3) SC-23(4)</keyword>
<keyword word="SESSIONS">AC-10 AC-12 AC-12(1) AC-17(1) AC-17(2) AC-2(6) MA-4 MA-4(1) MA-4(4) MA-4(5) MA-4(7) SC-10 SC-15(4) SC-2(1) SC-23 SC-23(5) SC-7(8) SI-14</keyword>

Key Word Lock

<keyword word="LOCK">AC-11 AC-11(1) AC-7(1)</keyword>

Any key words can be searched – used for multiple cases / inputs
How to reduce Time and Resources - 4 of 5

4th Step

Matching Key Words from Nessus Scans to IA Controls Using Fuzzy Logic / Ontology Approach

Nessus Scan in an XML Format

IA Controls in an XML Format

“Session”

CPE – Cisco, Juniper, MS
CVE
CVSS 2.9
1 - 3 Low, 4 – 7 M 8 – 9 H

CPE – Cisco, Juniper, MS
CVE
CVSS 5.9

CPE – Cisco, Juniper, MS
CVE
CVSS 1.0

RISK?
How to reduce Time and Resources - 4 of 5

4th Step

Matching Key Words from Nessus Scans to IA Controls Using Fuzzy Logic / Ontology Approach

ontology/symantec=fuzzy logic

Nessus Scan in an XML Format

IA Controls in an XML Format

Ontology/Symantec=Fuzzy Logic
How to reduce Time and Resources - 5 of 5

5th Step  
**Showing Results and Validating**

<table>
<thead>
<tr>
<th>Key Words</th>
<th>CVE</th>
<th>IA Controls</th>
<th>YES</th>
<th>NO</th>
</tr>
</thead>
<tbody>
<tr>
<td>Session</td>
<td>CVE – 2003-0011</td>
<td>AC-1</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>CVE – 2003-0023</td>
<td>AC-1</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Session</td>
<td>CVE – 2004-0012</td>
<td>AC-1</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Session</td>
<td>CVE – 2004-0056</td>
<td>AC-2</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td>Session</td>
<td>CVE – 2006-0087</td>
<td>AC-2</td>
<td></td>
<td>X</td>
</tr>
<tr>
<td>Session</td>
<td>CVE – 2008-0032</td>
<td>AC-2</td>
<td></td>
<td>X</td>
</tr>
</tbody>
</table>

Prepare the results to go into a POA&M

POA&M Converted into XML, CSV, Word Format
Situational Awareness of POA&M's Progress

Roll up counts of findings and remediated POA&M

<table>
<thead>
<tr>
<th>Controls</th>
<th>Count of Finding</th>
<th>Count Remediated</th>
</tr>
</thead>
<tbody>
<tr>
<td>AC-1</td>
<td>2</td>
<td>1</td>
</tr>
<tr>
<td>AC-2</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>AC-3</td>
<td>4</td>
<td>2</td>
</tr>
</tbody>
</table>

Unit 1
7 C&A Packages

Unit 2
3 C&A Packages

Unit 3
5 C&A Packages

Headquarters

Vulnerability Management Process
Manage FISMA