



The U.S. Cyber Security Framework: Intel's Lessons Learned

Tim Casey
Senior Strategic Risk Analyst
@timcaseycyber

SDN Cybersecurity Framework Training – May 2016



 How would you represent your entire risk landscape to your senior management?

 And how would you get there?

CSF Pilot @ Intel
March → Aug 2014

Additional assessments 2015+



Information Technology  3

Laying the Groundwork

Several methods to build comprehensive risk picture tried in the past, but none were satisfactory

Intel actively involved with NIST and CSF from beginning (February 2013)

Team engaged and educated senior management at very beginning

Also engaged other stakeholders early; their buy-in helped with resourcing

Interestingly, the Framework itself facilitated the discussions



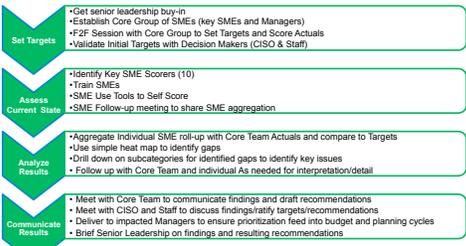
Framework Elements Support Common Understanding



The diagram illustrates how the five framework elements (Identify, Protect, Detect, Respond, Recover) are mapped across four tiers of maturity. A 'TARGET' bar chart shows the relative emphasis on each element for each tier: Tier 1 (Partial) focuses on Identify and Recover; Tier 2 (Risk-informed) adds Detect; Tier 3 (Repeatable) adds Protect; Tier 4 (Adaptive) includes all elements.



Intel's Framework Utilization Process



- Set Targets**
 - Get senior leadership buy-in
 - Establish Core Group of SMEs (key SMEs and Managers)
 - F2F Session with Core Group to Set Targets and Score Actuals
 - Validate Initial Targets with Decision Makers (CISO & Staff)
- Assess Current State**
 - Identify Key SME Scopers (10)
 - Train SMEs
 - SME Use Tools to Self Score
 - SME Follow-up meeting to share SME aggregation
- Analyze Results**
 - Aggregate Individual SME roll-up with Core Team Actuals and compare to Targets
 - Use simple heat map to identify gaps
 - Drill down on subcategories for identified gaps to identify key issues
 - Follow up with Core Team and individual As needed for interpretation/detail
- Communicate Results**
 - Meet with Core Team to communicate findings and draft recommendations
 - Meet with CISO and Staff to discuss findings/ratify targets/recommendations
 - Deliver to impacted Managers to ensure prioritization feed into budget and planning cycles
 - Brief Senior Leadership on findings and resulting recommendations



Setting the Targets

Category	Actual	Target	Delta
Identity	3	3	0
Business Environment	2	2	0
Risk Management	2	2	0
Information	2	2	0
Risk Assessment	2	2	0
Risk Management Strategy	2	2	0
Process	2	2	0
System Control	2	2	0
Access Control	2	2	0
Network Security	2	2	0
Physical Access & Perimeters	2	2	0
Monitoring	2	2	0
Incident Response	2	2	0
Defect	2	2	0
Business Continuity	2	2	0
Security Continuous Monitoring	2	2	0
Business Process	2	2	0
Response	2	2	0
Business Planning	2	2	0
Business	2	2	0
Compliance	2	2	0
Regulation	2	2	0
Recovery	2	2	0
Business Continuity	2	2	0
Information Security	2	2	0
Information Systems	2	2	0

The Core Team, made of managers and lead SMEs, collectively assessed risk tolerance for each category

SME Scoring

Category	Policy	Network	Endpoint/Device	Identity	App	Regn	Self Rate
Identity	3	3	3	3	3	3	3
Business Environment	2	2	2	2	2	2	2
Risk Management	2	2	2	2	2	2	2
Information	2	2	2	2	2	2	2
Risk Assessment	2	2	2	2	2	2	2
Risk Management Strategy	2	2	2	2	2	2	2
Process	2	2	2	2	2	2	2
System Control	2	2	2	2	2	2	2
Access Control	2	2	2	2	2	2	2
Network Security	2	2	2	2	2	2	2
Physical Access & Perimeters	2	2	2	2	2	2	2
Monitoring	2	2	2	2	2	2	2
Incident Response	2	2	2	2	2	2	2
Defect	2	2	2	2	2	2	2
Business Continuity	2	2	2	2	2	2	2
Security Continuous Monitoring	2	2	2	2	2	2	2
Business Process	2	2	2	2	2	2	2
Response	2	2	2	2	2	2	2
Business Planning	2	2	2	2	2	2	2
Business	2	2	2	2	2	2	2
Compliance	2	2	2	2	2	2	2
Regulation	2	2	2	2	2	2	2
Recovery	2	2	2	2	2	2	2
Business Continuity	2	2	2	2	2	2	2
Information Security	2	2	2	2	2	2	2
Information Systems	2	2	2	2	2	2	2

Mapping highlighted outliers and major differences

Our Final Result

Category	Actual	Target	Delta
Identity	3	3	0
Business Environment	2	2	0
Risk Management	2	2	0
Information	2	2	0
Risk Assessment	2	2	0
Risk Management Strategy	2	2	0
Process	2	2	0
System Control	2	2	0
Access Control	2	2	0
Network Security	2	2	0
Physical Access & Perimeters	2	2	0
Monitoring	2	2	0
Incident Response	2	2	0
Defect	2	2	0
Business Continuity	2	2	0
Security Continuous Monitoring	2	2	0
Business Process	2	2	0
Response	2	2	0
Business Planning	2	2	0
Business	2	2	0
Compliance	2	2	0
Regulation	2	2	0
Recovery	2	2	0
Business Continuity	2	2	0
Information Security	2	2	0
Information Systems	2	2	0

Our Key Learnings

- The CSF **fosters essential internal discussions** about alignment, risk tolerance, control maturity, and other elements of cyber risk management
 - Setting our own Tier Targets was especially useful
- The CSF provides a **common language** for cross-organizational communications, allowing apple-to-apples comparisons
- Engage all stakeholders early; the **Framework itself facilitates discussion**
- Its **alignment to industry practices** made it easy to scale and tailor it to our environment with surprisingly minimal impact



Information Technology



Utilizing the Framework in Your Organization

You will miss the benefits if you treat the Framework as a compliance exercise, or use an outside agency do it for you
 → Coaching is fine but *you need to make the journey yourself*



First: Inform senior management on the Framework and benefits:

- Driven by and follows industry best practices
- Provides common a cybersecurity reference up and down the organization
- Drives important conversations on your risks and your tolerance
- Can lead to a much better understanding of your complete risk picture

Information Technology



Resources

Intel CSF white paper: <http://www.intel.com/content/www/us/en/government/cybersecurity-framework-in-action-use-case-brief.html>

NIST CSF Website: <http://www.nist.gov/cyberframework>

U.S. Sector Information Sharing & Analysis Centers (ISAC): <http://www.isaccouncil.org/home.html>

U.S. Dept. Homeland Security Critical Infrastructure Cyber Community (C³) Voluntary Program: <http://www.dhs.gov/about-critical-infrastructure-cyber-community-c%C2%B3-voluntary-program>

Intel Threat Agent Analysis: <https://communities.intel.com/docs/DOC-23914>
<https://communities.intel.com/docs/DOC-1151>

We engage with fellow travelers and communities utilizing the CSF related to:

- Threat Assessments
- Supplier Management and Supply Chain Risk
- Manufacturing / ICS Risk
- Tools and Visualization

Information Technology



Questions?

Tim Casey@Intel.com
@timcasey cyber



This presentation is for informational purposes only.
INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS AND SERVICES. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.
Intel, the Intel logo, Look Inside, and the Look Inside logo are trademarks of Intel Corporation in the U.S. and/or other countries.
Other names and brands may be claimed as the property of others.
Copyright © 2016 Intel Corporation. All rights reserved.
