



Cyber Security Framework: Intel's Implementation Tools & Approach

Tim Casey
Senior Strategic Risk Analyst
@timcaseycyber

NIST Workshop #6

October 29, 2014



Intel's Goals in Using the CSF

- Establish alignment on risk tolerance
- Inform budget planning for 2015
- Communicate risk heat map to Senior Leadership
- CSF as risk management approach – NOT a compliance checklist!

Strategy: 3-Phase Approach

Infrastructure

- Align Macro-level risk management practices to CSF
- Focus initially on OFFICE and ENTERPRISE
- Perform initial CSF assessment against infrastructure

← We are here

Product

- Explore mapping of products and services capabilities to CSF
- Examine product assurance initiatives (SDL, etc.) through CSF lens

Supply Chain/Third Party Contracting

- Examine and potentially pilot contracting updates to align to CSF language

Infrastructure Assessment Process

Set Targets

- Establish **Core Group** (key SME's and Managers)
- **Evaluate and modify Categories and Subcategories**
- F2F Session with Core Group to **set targets and score actuals** (2x4 hour sessions/8-10 SME's)
- **Validate Targets** with Decision Makers (CISO & Staff)

Assess Current State

- Identify Key **SME Scorers**
- **Train SMEs** (virtual 1 hour sessions)
- SME Use Tools to **self score** [note: SME's do not know Targets]

Analyze Results

- **Aggregate** Individual SME roll-up with Core Team Actuals and **compare to Targets**
- Use simple heat map to **identify gaps** >1
- Drill down on subcategories for identified gaps >1 to **identify key issues**

Communicate Results

- **Review** findings & recommendations with **CISO & Staff**
- **Inform impacted Managers** to ensure prioritization feed into budget and planning cycles
- **Brief Senior Leadership** on findings and resulting recommendations

SME Rollup

	Policy	Network	Endpoint/ Data Protection	Identity	Ops	Apps	SME Ave
3	Identify						
4	Business Environment	3	3	2	3	2	3
5	Asset Management	3	2	2	1	3	2
6	Governance	3	2	3	2	2	2
7	Risk Assessment	2	2	2	2	3	2
8	Risk Management Strategy	4	3	2	2	2	3
9	Protect						
10	Access Control	2	3	3	2	3	3
11	Awareness/Training	2	3	3	2	3	3
12	Data Security	2	2	2	2	2	2
13	Protective Process and Procedures	2	3	3	1	2	2
14	Maintenance	NA	2	2	2	4	2
15	Protective Technologies	NA	2	1	3	1	2
16	Detect						
17	Anomalies/Events	2	3	1	2	4	2
18	Security Continuous Monitoring	2	2	1	2	1	1
19	Detection Process	2	3	2	2	3	2
20		NA	3	3	NA	2	3
21		2	2	3	2	3	3
22		2	2	3	2	3	3
23	Analysis	2	3	2	3	3	3
24	Mitigations	2	3	2	3	1	2
25	Improvements	3	3	3	2	2	2
26	Recover						
27	Recovery Planning	2	3	3	2	3	3
28	Improvements	1	3	2	1	3	2
29	Communications	2	2	3	2	3	2

Mapping highlighted outliers and major differences

NOTIONAL / EXAMPLE ONLY

SME-Core Target Roll Up

1		SME Ave	Core Team	Combined Score	Target	Risk Gap
2	Identify					
3	Business Environment	3	2	2	3	1
4	Asset Management	2	3	3	3	0
5	Governance	2	2	2	2	0
6	Risk Assessment	2	1	2	3	1
7	Risk Management Strategy	3	2	2	4	2
8	Protect					
9	Access Control	3	2	2	3	1
10	Awareness/Training	3	3	3	4	1
11	Data Security	2	3	3	3	0
12	Protective Process and Procedures	2	2	2	4	2
13	Maintenance	2	1	2	3	1
14	Protective Technologies	2	3	2	3	1
15	Detect					
16	Anomalies/Events	2	2	2	4	2
17	Security Continuous Monitoring	1	2	2	4	2
18	Detection Process	2	3	3	3	0
19	Threat Intelligence	3	3	3	3	0
20	Respond					
21	Response Planning	3	2	2	4	2
22	Communication	3	1	2	3	1
23	Analysis	3	2	2	3	1
24	Mitigations	2	3	3	3	0
25	Improvements	2	1	2	2	0
26	Recover					
27	Recovery Planning	3	3	3	3	0
28	Improvements	2	1	2	2	1
29	Communications	2	3	3	3	0

Significant differences between Core and Individual scores can highlight visibility issues

High 2's – Focus Areas stand out

Results matched “Gut Check” expectations

NOTIONAL / EXAMPLE ONLY

Management Outcomes

Program Management

- CSF utilization has progressed with no major deviations from plan of record
- Very light-weight organizationally—leveraged existing processes & org structures

Estimated Cost

- Less than **150 work-hours** invested to date with 2 focus areas (Office & Enterprise) complete
- Repeatable tools & techniques developed so additional areas may be less overhead

Feedback from Participants

- Easy to understand and score
- No push back on resourcing or time commits
- Participants see value, with key concerns being granularity and repeatability

Key Learnings

Setting Targets is a very valuable exercise

- Discussions on Tiers and Targets was enlightening and furthered intra-company alignment

Categories

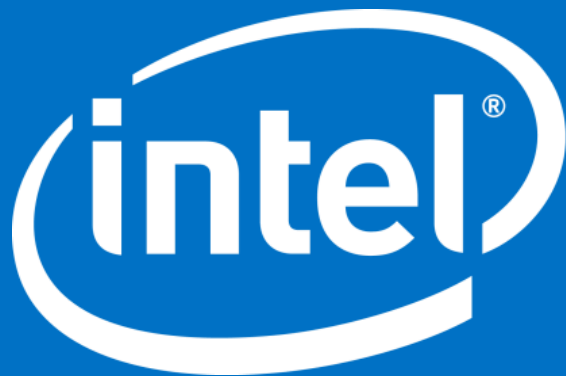
- Categories were useful and for our initial use only one additional Category added – DETECT: THREAT INTELLIGENCE
- We expect additional Categories to emerge as we move through Design, Manufacturing, and Services environments

Sub Categories

- Still a bit of a puzzle on how to optimally use this granularity while balancing overhead
- Next rev of tool will do away with scoring subcategories and use over/under model for heat mapping inputs

Summary

- “This is a journey.” Informed internal discussion is a key aspect of any risk management program—the CSF fosters this well
- For Intel, a relatively low-cost and low-impact process modification
- Improved harmonization of risk management methodologies and a common language across internal stakeholder communities
- Improved visibility into our risk landscape



This presentation is for informational purposes only. INTEL MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS SUMMARY.

BunnyPeople, Celeron, Celeron Inside, Centrino, Centrino Inside, Core Inside, i960, Intel, the Intel logo, Intel AppUp, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, the Intel Inside logo, Intel NetBurst, Intel NetMerge, Intel NetStructure, Intel SingleDriver, Intel SpeedStep, Intel Sponsors of Tomorrow., the Intel Sponsors of Tomorrow. logo, Intel StrataFlash, Intel Viiv, Intel vPro, Intel XScale, InTru, the InTru logo, InTru soundmark, Itanium, Itanium Inside, MCS, MMX, Moblin, Pentium, Pentium Inside, skool, the skool logo, Sound Mark, The Journey Inside, vPro Inside, VTune, Xeon, and Xeon Inside are trademarks of Intel Corporation in the U.S. and other countries.

*Other names and brands may be claimed as the property of others.

Copyright © 2014, Intel Corporation. All rights reserved.