Intel Security and Privacy Office

Protecting to Enable People, Data & Business

intel Look Inside.™

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

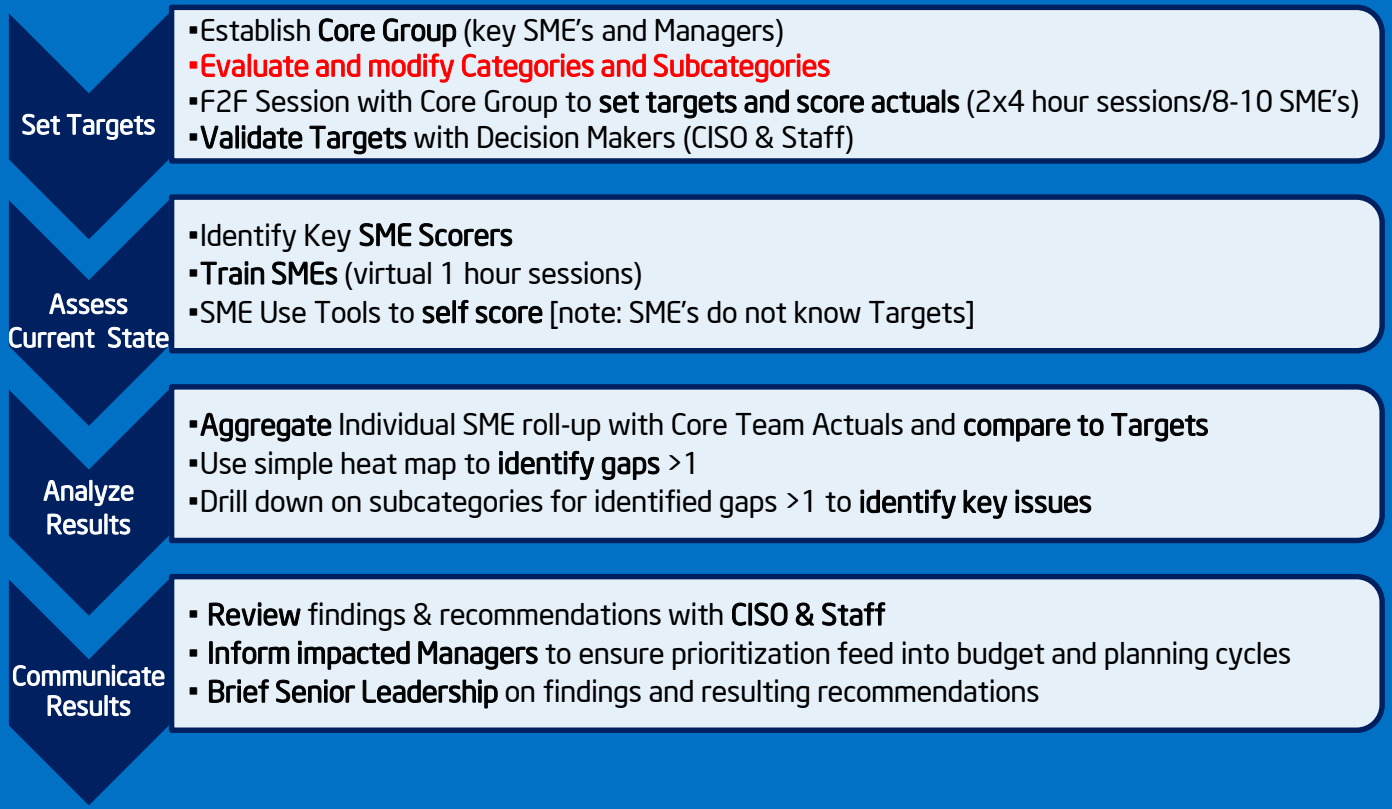
Product

- 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



SME Rollup

	Policy	Network	Endpoint/ Data Protection	Identity	Ops	Apps	SME Ave
Identify							
Business Environment	3	3	3	2	3	2	3
Asset Management	3	2	2	2	1	3	2
Governance	3	2	3	2	2	2	2
Risk Assessment	2	2	2	2	2	3	2
Risk Management Strategy	4	3	2	2	2	2	3
Protect							
Access Control	2	3	3	2	3	2	3
Awareness/Training	2	3	3	2	3	3	3
Data Security	2	2	2	2	2	2	2
Protective Process and Procedures	2	3	3	1	2	2	2
Maintenance	NA	2	2	2	2	4	2
Protective Technologies	NA	2	1	3	1	2	2
Detect							
Anomolies/Events	2	3	1	2	3	4	2
Secruity Continous Monitoring	2	2	1	2	1	1	1
Detection Process	2	3	2	2	3	2	2
	NA	3	3	NA	2	2	3
	2	2	3	2	3	2	3
	2	2	3	2	2	3	3
Analysis	2	3	3	2	3	3	3
Mitigations	2	3	1	2	3	1	2
Improvements	3	3	3	3	2	2	2
Recover							
Recovery Planning	2	3	3	2	2	3	3
Improvements	1	3	2	1	2	3	2
Communications	2	2	3	2	1	3	2

Mapping highlighted outliers and major differences

NOTIONAL / EXAMPLE ONLY

SME-Core Target Roll Up

	SME Ave	Core Team	Combined Score	Target	Risk Gap
Identify					
Business Environment	3	2	2	3	1
Asset Management	2	3	3	3	0
Governance	2	2	2	2	0
Risk Assessment	2	1	2	3	1
Risk Management Strategy	3	2	2	4	2
Protect					
Access Control	3	2	2	3	1
Awareness/Training	3	3	3	4	1
Data Security	2	3	3	3	0
Protective Process and Procedures	2	2	2	4	2
Maintenance	2	1	2	3	1
Protective Technologies	2	3	2	3	1
Detect					
Anomolies/Events	2	2	2	4	2
Secruity Continous Monitoring	1	2	2	4	2
Detection Process	2	4	3	3	0
Threat Intelligence	3	3	3	3	0
Respond					
Response Planning	3	2	2	4	2
Communication	3	1	2	3	1
Analysis	3	2	2	3	1
Mitigations	2	3	3	3	0
Improvements	2	1	2	2	0
Recover					
Recovery Planning	3	3	3	3	0
Improvements	2	1	2	2	1
Communications	2	3	3	3	0

NOTIONAL / EXAMPLE ONLY

Significant differences between Core and Individual scores can highlight visibility issues

High 2's – Focus Areas stand out

Results matched "Gut Check" expectations

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