

# RSA® Conference 2015

San Francisco | April 20-24 | Moscone Center

SESSION ID: STR-W01

## Implementing the U.S. Cybersecurity Framework at Intel—A Case Study

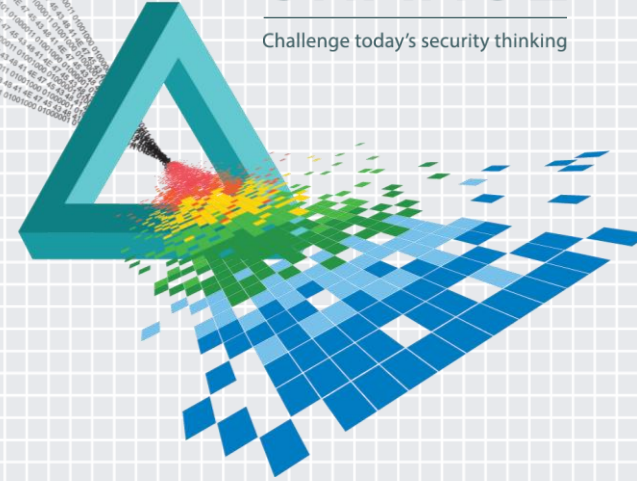
**Tim Casey**

---

Senior Strategic Risk Analyst  
Intel Information Security  
@timcaseycyber

# CHANGE

Challenge today's security thinking





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



**And how would you get there?**

## Topics

Our goals & strategy for the CSF

Framework structures we used

Pilot implementation & results

Key Learnings

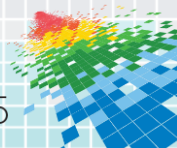
Our Recommendations

## *Not Covered*

*CSF development / management*

*CSF 2.0*

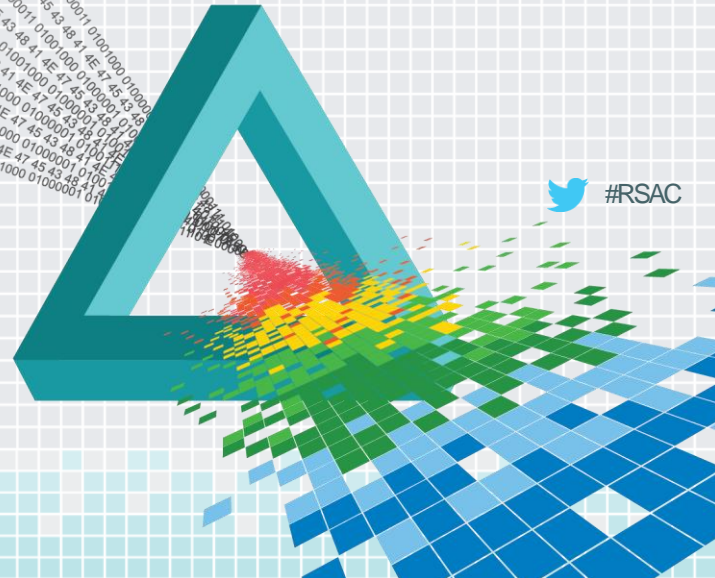
*Regulatory concerns*



# RSA<sup>®</sup>Conference2015

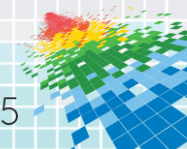
San Francisco | April 20-24 | Moscone Center

## The Cybersecurity Framework Basics



# Framework Core

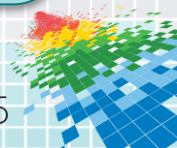
Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT			
DETECT			
RESPOND			
RECOVER			



# Framework Core

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT	Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational		
DETECT			
RESPOND			
RECOVER			

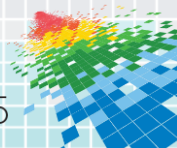
Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational confidentiality, integrity, and availability requirements.



# Framework Core

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT	Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational	PR.DS-1: Protect data (including phys records) during storage to achieve	
DETECT			
RESPOND			
RECOVER			

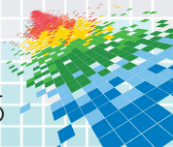
PR.DS-1: Protect data (including physical records) during storage to achieve confidentiality, integrity, and availability goals



# Framework Core

Framework Core			
Functions	Categories	Subcategories	References
IDENTIFY			
PROTECT	Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational	PR.DS-1: Protect data (including phys records) during storage to achieve	COBIT APO01.06, BAI02.01 ISO/IEC 27001 A.15.1.3
DETECT			
RESPOND			
RECOVER			

- COBIT APO01.06, BAI02.01
- ISO/IEC 27001 A.15.1.3
- CCS CSC 17
- NIST SP 800-53 Rev 4 SC-28





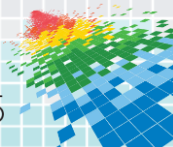
# Framework Tiers & Profiles

## Tier Definitions

### Tiers

**Tier 4: *Adaptive***  
**Tier 3: *Repeatable***  
**Tier 2: *Risk-Informed***  
**Tier 1: *Partial***

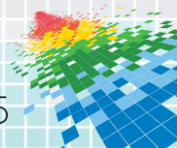
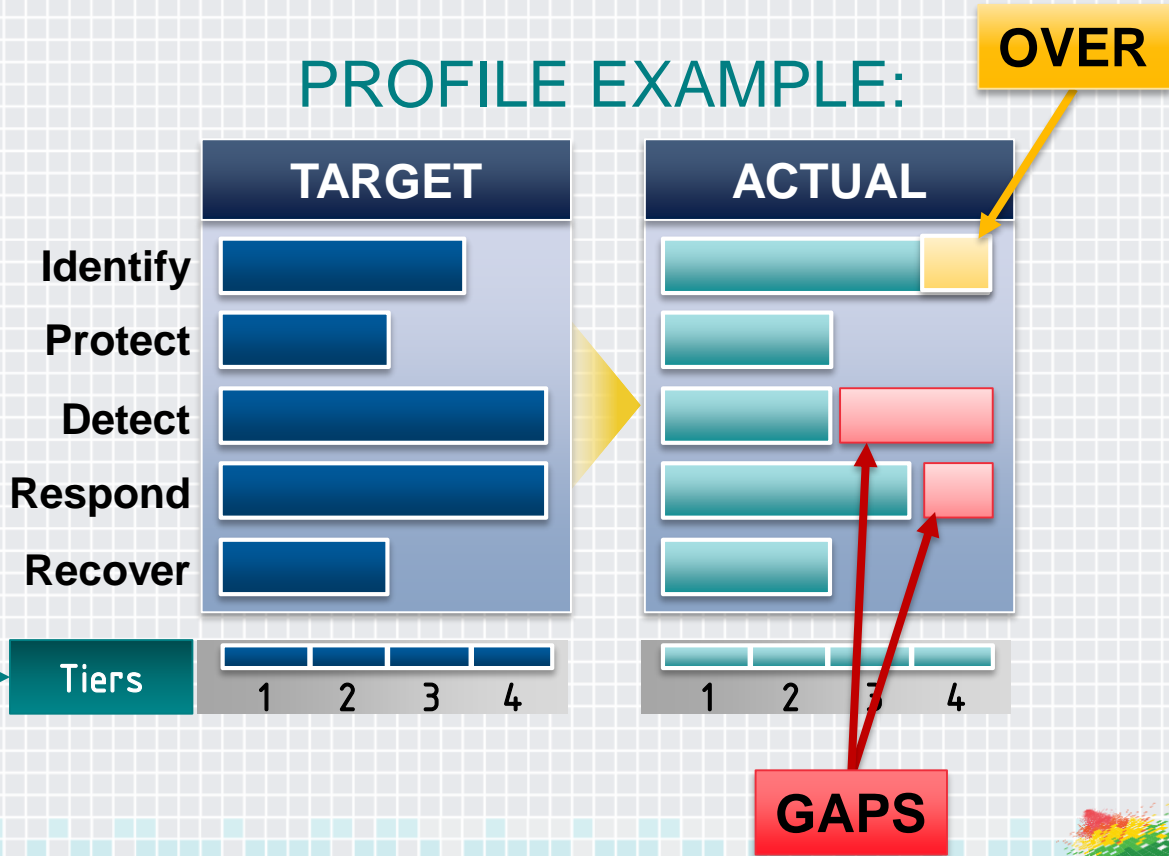
	Score 1 - Partial	Score 2 - Risk Informed	Score 3 - Repeatable	Score 4 - Adaptive
People	Staff has had minimal cybersecurity-related training. There is limited or non-existent training pipeline for security staff. Security awareness is limited. Staff has non-existent or limited awareness of Intel Security resources and escalation paths.	Employees have received cybersecurity-related training. There is a training pipeline for security staff and personnel. There is an awareness of cybersecurity risk at the organizational level. Employees have a general awareness of security and Intel Security resources and escalation paths.	Personnel possess the knowledge and skills to perform their appointed roles and responsibilities. Employees receive regular cybersecurity-related training and briefings. There is a robust training pipeline for security staff and personnel. Employees attend internal and external security conferences or training opportunities. Organization has a Security Champion or dedicated security personnel.	People: Personnel knowledge and skills are regularly reviewed for currency and applicability and new skills and knowledge needs identified and addressed... Employees receive regular cybersecurity-related training and briefings on relevant and emerging security topics. There is a robust training pipeline for security staff and personnel. Employees routinely attend internal and external security conferences or training opportunities.
Process	Risk management process not formalized. Risks are managed in a reactive, ad hoc manner. Business decision and/or prioritization do not factor in risk and/or threat assessments. Risk and threat information is not communicated to internal stakeholders.	Prioritization of cybersecurity activities is directly informed by organizational risk objectives, the threat environment, or business/mission requirements. Risk-informed, management-approved processes and procedures are defined and implemented, and staff has adequate resources to perform their cybersecurity duties. Cybersecurity information is shared within the organization on an informal basis. Risk management practices are approved by management but may not be established as organizational-wide policy.	Organizational cybersecurity practices are regularly updated based on the application of risk management processes to changes in business/mission requirements and a changing threat and technology landscape. Risk management practices are formally approved and expressed as policy and there is an organization-wide approach to manage cybersecurity risk. Risk-informed policies, processes, and procedures are defined, implemented as intended, and reviewed. Consistent methods are in place to respond effectively to changes in risk.	The organization adapts its cybersecurity practices based on lessons learned and predictive indicators derived from previous and current cybersecurity activities. Through a process of continuous improvement incorporating advanced cybersecurity technologies and practices, the organization actively adapts to a changing cybersecurity landscape and responds to evolving and sophisticated threats in a timely manner. There is an organization-wide approach to managing cybersecurity risk that uses risk-informed policies, processes, and procedures to address potential cybersecurity events. Cybersecurity risk management is part of the organizational culture and evolves from an awareness of previous activities, information shared by other sources, and continuous awareness of activities on their systems and networks.
Technology	Tools are not deployed, not supported or insufficient to address risks. Tools may be in place but are not adequately tuned or maintained. Technology deployed lags current threats. Tool coverage lacking (tool is deployed in a limited way).	Tools are deployed and supported to address identified risks. Tools in deployment are routinely tuned and/or maintained. Technology deployed, for the most part, paces current threats. Tool coverage of the risk area is complete.	Metrics are used to evaluate the usefulness and effectiveness of deployed tools. Tools in deployment are tuned and/or maintained. Technology deployed paces current and emerging threats. Tool coverage of the risk area is complete and as new infrastructure is deployed, tool coverage is addressed.	Tools deployed in the environment are regularly reviewed for effectiveness and coverage against changes in threat environment and internal ecosystem. Tools and technology deployed anticipates emerging threats.
Ecosystem	Organization does not know its role in the larger ecosystem. Organization does not have processes in place to participate in or collaborate with external organizations.	The organization knows its role in the larger ecosystem but has not formalized its capabilities to interact and share information externally.	The organization understands its dependencies and partners and receives information from these partners that enables collaboration and risk-based management decisions within the organization in response to events.	The organization manages risk and actively shares information with partners to ensure that accurate, current information is being distributed and consumed to improve cybersecurity before a cybersecurity event occurs.



# Framework Tiers & Profiles

## Tiers

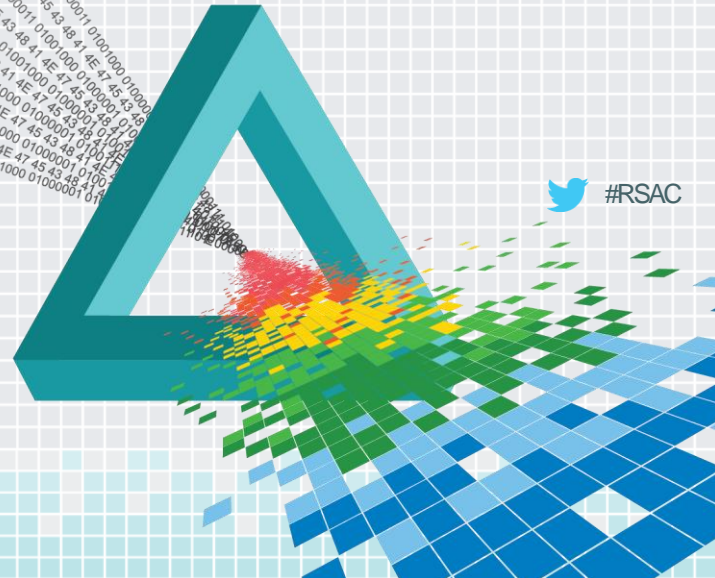
- Tier 4: *Adaptive*
- Tier 3: *Repeatable*
- Tier 2: *Risk-Informed*
- Tier 1: *Partial*



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

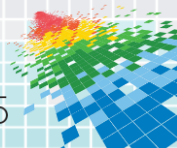
## Intel's Cybersecurity Framework Pilot



 #RSAC

# 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) and ready to pilot at release
- ◆ 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



# Pilot Scope (or, Eating the Elephant)

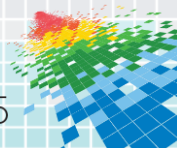
- Intel is a large multi-national enterprise with many business units and 300k+ computing platforms— and,
- The Framework has ~140 potential assessment points

*Just designing a pilot to cover all that could take months*

**So—**

Decision made up front to pilot on a **subset** of well-defined areas

- ◆ Not expecting entire risk management plan from just a pilot
- ◆ Simplified pilot assessment allows us to focus on CSF usage, not implementation details




# Pilot Scoping – Subset of the Company

- ◆ IT models support across company as *DOMES*—  
***Design, Office, Manf., Enterprise, Services***
- ◆ Pilot w/ *Office + Enterprise*
  - ◆ IT-owned
  - ◆ Highest familiarity with Core Team

	Design	Office	Manufacturing	Enterprise	Services
<b>Identify</b>					
Business Environment					
Asset Management					
Governance					
Risk Assessment					
Risk Management Strategy					
<b>Protect</b>					
Access Control					
Awareness/Training					
Data Security					
Protective Process & Procedures					
Maintenance					
Protective Technologies					
<b>Detect</b>					
Anomalies/Events					
Security Continuous Monitoring					
Detection Process					
Threat Intelligence					
<b>Respond</b>					
Response Planning					
Communication					
Analysis					
Mitigations					
Improvements					
<b>Recover</b>					
Recovery Planning					
Improvements					
Communications					

Focus Areas



# Pilot Scoping – Only the Top Level of the CSF

- ◆ Assessing subcategories too large a task for a pilot
- ◆ Decided to only assess to **Category** level (21+1)
- ◆ Our training covered how to assess to higher level

Framework Core			
Functions	Categories	Subcategories	Informative References
IDENTIFY			
PROTECT	Data Security (DS): Protect information & data from natural and man-made hazards to achieve organizational		
DETECT			
RESPOND			
RECOVER			

# Framework Utilization Process

## Set Targets

- Tailor Tiers definitions
- F2F Session with Core Group to set Targets (Category level)
- Validate Initial Targets with Decision Makers (CISO & Staff)

## Assess Current State

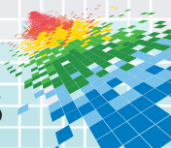
- Identify and train SME assessors
- SMEs use custom tools to self score (~1 hour)
- Follow-up meeting to validate SME aggregation

## Analyze Results

- Combine individual SME scores with Core Team and compare to Targets
- Use simple heat map to identify gaps
- Drill down on subcategories for identified gaps to identify key issues

## Communicate Results

- Meet with CISO & Staff to discuss findings, ratify targets & recommendations
- Ensure prioritization feed into budget and planning cycles
- Brief Senior Leadership on findings and resulting recommendations

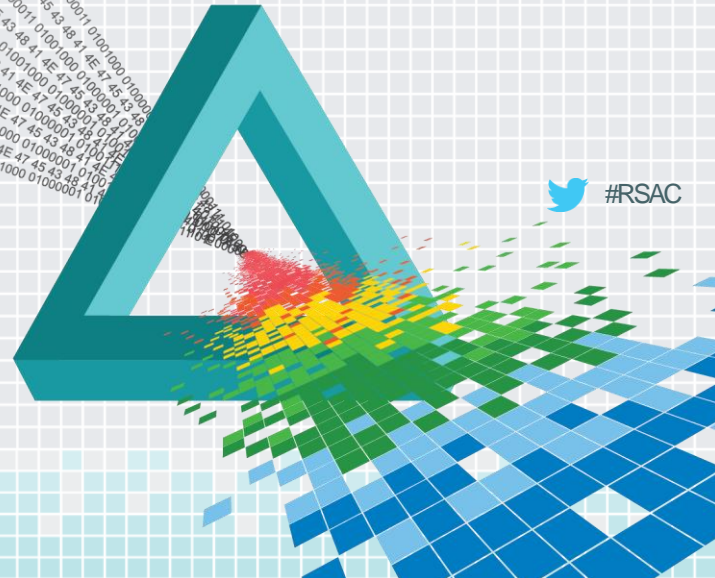




# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Results

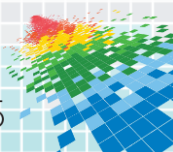


# Unexpected Benefits: SME Roll-up

	Policy	Network	Endpoint/ Data Protection	Identity	Ops	Apps	SME Ave	
2								
3	<b>Identify</b>							
4	Business Environment	3	3	3	2	3	2	3
5	Asset Management	3	2	2	2	1	3	2
6	Governance	3	2	3	2	2	2	2
7	Risk Assessment	2	2	2	2	2	3	2
8	Risk Management Strategy	4	3	2	2	2	2	3
9	<b>Protect</b>							
10	Access Control	2	3	3	2	3	2	3
11	Awareness/Training	2	3	3	2	3	3	3
		2	2	2	2	3	2	2
		2	3	3	1	2	2	2
		2	2	2	2	2	4	2
		2	2	1	3	1	2	2
16	<b>Detect</b>							
17	Anomalies/Events	2	3	1	2	2	4	2
18	Security Continuous Monitoring	2	2	1	2	1	1	1
19	Detection Process	2	3	2	2	3	2	2
20	Threat Intelligence	2	3	3	2	2	2	3
21	<b>Respond</b>							
22	Response Planning	2	2	3	2	3	2	3
23	Communication	2	2	3	2	2	3	3
24	Analysis	2	3	3	2	3	3	3
25	Mitigations	2	3	1	2	3	1	2
26	Improvements	3	3	3	3	2	2	2
27	<b>Recover</b>							
28	Recovery Planning	2	3	3	2	2	3	3
29	Improvements	1	3	2	1	2	3	2
30	Communications	2	2	3	2	1	3	2

Evaluating by functional area provided greater insights

NOTIONAL / EXAMPLE ONLY



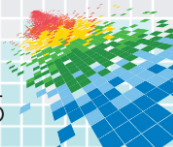
# Unexpected Benefits: SME Roll-up

	Policy	Network	Endpoint/ Data Protection	Identity	Ops	Apps	SME Ave
<b>Identify</b>							
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
<b>Protect</b>							
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	3	2
13	Protective Process and Procedures	2	3	3	1	2	2
14	Maintenance	2	2	2	2	2	4
15	Protective Technologies	2	2	1	3	1	2
<b>Detect</b>							
17	Monitoring	2	3	1	2	2	4
18	Incident Response	2	2	1	2	1	1
19	Threat Intelligence	2	3	2	1	3	2
20	Log Management	2	3	3	2	2	3
<b>Respond</b>							
22	Response Planning	2	2	3	2	3	3
23	Communication	2	2	3	2	2	3
24	Analysis	2	3	3	2	3	3
25	Mitigations	2	3	1	2	3	2
26	Improvements	3	3	3	3	3	3
<b>Recover</b>							
28	Recovery Planning	2	3	3	2	3	3
29	Improvements	1	3	2	1	3	2
30	Communications	2	2	3	2	1	2

Highlight outliers

Highlight major differences

NOTIONAL SAMPLE ONLY

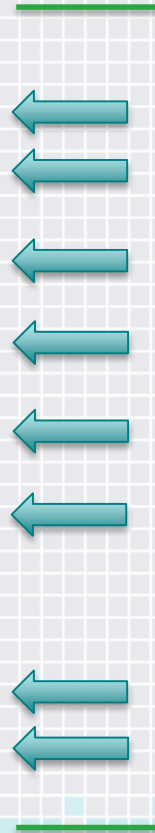


# Our Final Result



NOTIONAL / EXAMPLE ONLY

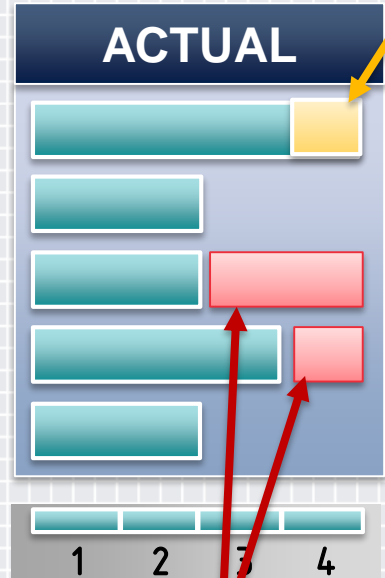
Category	Actual	Target	Delta
<b>Identify</b>	3	3	0
Business Environment	2	2	0
Asset Management	2	2	0
Governance	4	3	1
Risk Assessment	2	2	0
Risk Management Strategy	2	4	-2
<b>Protect</b>	2	2	0
Access Control	1	1	0
Awareness/Training	2	3	-1
Data Security	2	2	0
Protective Process & Procedures	2	2	0
Maintenance	3	4	-1
Protective Technologies	2	2	0
<b>Detect</b>	1	1	0
Anomalies/Events	3	2	1
Security Continuous Monitoring	4	4	0
Detection Process	2	2	0
Threat Intelligence	3	4	-1
<b>Respond</b>	2	2	0
Response Planning	1	1	0
Communication	3	3	0
Analysis	2	2	0
Mitigations	2	2	0
Improvements	3	4	-1
<b>Recover</b>	3	3	0
Recovery Planning	2	4	-2
Improvements	2	2	0
Communications	4	4	0



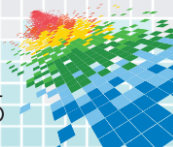
## THE RISK LANDSCAPE!



**OVER**



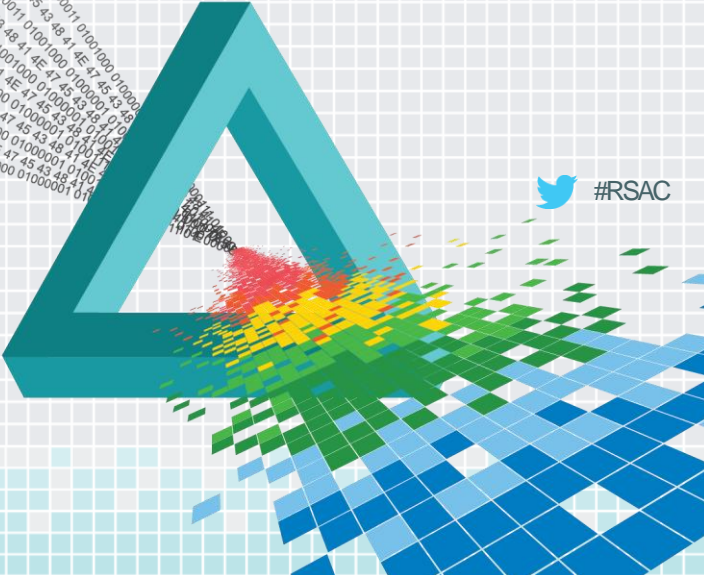
**GAPS**



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

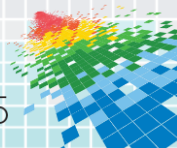
## Summary



 #RSAC

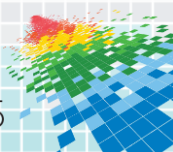
# Our Key Learnings

- ◆ 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



# Challenges

- ◆ Since this is a new tool, both management and pilot participants needed extra discussion up front to become comfortable with it
- ◆ For ease of use, we chose to tailor the Tiers definitions to match our own business and risk management language
- ◆ Subcategories provided almost overwhelming level of detail – still trying to figure out how to best leverage them

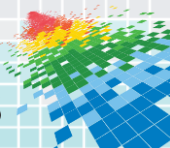


# Looking Ahead: Insider Risk and CSF

Intent →	Non-hostile			Non-Hostile / Hostile		Hostile							
	Reckless Employee	Untrained/Distracted Employee	Outward Sympath'zr	Vendor	Partner	Irrational Individual	Thief	Disgruntled Employee	Activist	Terrorist	Organized Crime	Competitor	Nation State
Accidental leak	X	X	X	X	X	X		X					
Espionage				X	X		X	X	X		X	X	X
Financial fraud				X	X		X	X			X		
Misuse	X	X	X	X	X	X		X	X				
Opport. data theft				X	X		X	X	X		X	X	X
Physical Theft						X	X	X		X	X		
Product alteration	X	X		X	X			X	X		X	X	X
Sabotage						X		X	X	X		X	X
Violence						X		X		X			

*Intel Threat Agent analysis of most-likely insider threats in a typical corporate environment*

Goal: Pilot using CSF to assess and characterize our Insider Risk





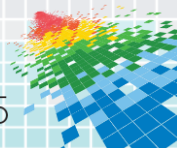
# Apply: Utilizing the CSF in Your Organization

**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



# Apply: Utilizing the CSF in Your Organization, cont'd

Next, engage and inform all your stakeholders

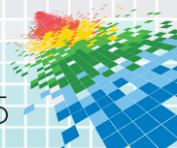
- ◆ Managers & SMEs in InfoSec, IT, GRC, Supply Chain, Finance...
- ◆ Cast a wide net; eventually many will have inputs
- ◆ Connect with partners & fellow travelers in your industry

With the stakeholders, design your pilot

- ◆ Start where you are comfortable
- ◆ Use a logical subset of your cybersecurity domain

Execute the pilot

- ◆ Maintain **constant** contact with senior management and stakeholders
- ◆ **Start with the Tiers & Targets discussions**, not mapping the categories
- ◆ Share your results!

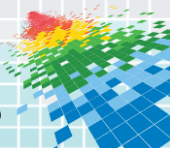


# Resources

- ◆ 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 (C<sup>3</sup>) 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 actively 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



# RSA<sup>®</sup>Conference2015

San Francisco | April 20-24 | Moscone Center

## Questions?

[Tim.Casey@intel.com](mailto:Tim.Casey@intel.com)

[@timcasey cyber](https://twitter.com/timcasey cyber)

