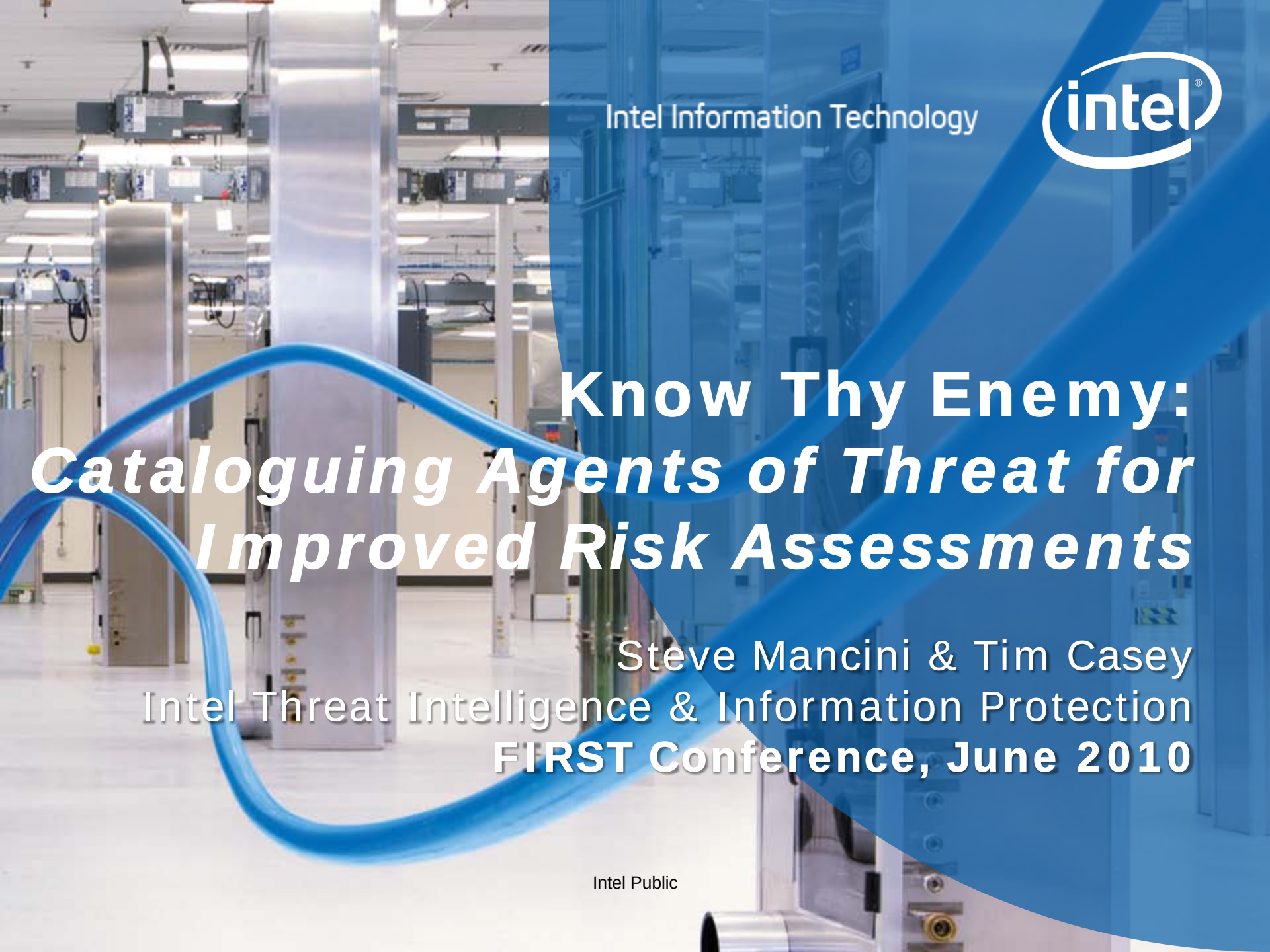


Intel Information Technology

Know Thy Enemy: *Cataloguing Agents of Threat for Improved Risk Assessments*

Steve Mancini & Tim Casey
Intel Threat Intelligence & Information Protection

FIRST Conference, June 2010

Objectives

- *Purpose of the Threat Agent Library (TAL)*
- *Threat Agent Taxonomy*
- *Using the Library*

Topics

- *Threat ID Problem*
- *Solution: TAL*
- *Building the Agents*
- *Using the Library*
- *Resources*

The Problem

- No coherent process existed to consistently identify and analyze the threat from human actors (“threat agents”) in information security risk assessments.
- No standardized and reusable method to describe the relative strengths and weaknesses of threat agents, which enables rational assessment of the level of controls needed.

Many hours spent negotiating the threat agents, with different results every time = wasted time and random results

Solution: Threat Agent Library

- Provides a catalog of agents, with defined strengths and weaknesses, to *consistently* and *repeatably* identify and analyze threat sources in information security risk assessments by providing a common framework
- Assists in assessing risk, but not to identify an actual attacker or attack in progress
- Fosters ongoing discussion, examination, and improvements in identifying and tracking types of threat

The Library covers the broadest possible spectrum of agents, applying equally to any country, environment, or industry.

Preview: Agents by Label

Hostile Agents

- Anarchist
- Civil Activist
- Competitor
- Corrupt Gov't Official
- Cyber Vandal
- Data Miner
- Employee, Disgruntled
- Government Spy
- Gov't Cyberwarrior
- Internal Spy
- Irrational Individual
- Legal Adversary
- Mobster
- Radical Activist
- Sensationalist
- Terrorist
- Thief
- Vendor

Non-Hostile Agents

- Employee, Distracted
- Employee, Reckless
- Employee, Untrained
- Information Partner

Threat Assessment Group: Innovation on a Shoestring Budget

- Started w/discussion around an idea, discussion became extended & formalized
- Not a formal project, no deadline or deliverables
- It was allowed to grow organically
  - A thought exercise that explored many avenues, some dead ends
  - Always an eye to producing something useful
  - Management was tolerant of organic approach because few resources spent
  - No expectation of reward other than our contribution to Intel security
- Worked around other schedules
  - Short hiatus at EOQ
  - Very tolerant of necessary absences (best effort)
- Membership held to those with genuine interest and desire to participate
  - Not dependant on any one person, true group effort
  - No one was assigned, all volunteered because they believed in project
  - Membership is fluid
  - Members are welcomed for what they bring, not exclusionary
  - Discussion was always civil but often quite vigorous

New Taxonomy: Threat Attributes

- **Access** – Insider access to facilities and networks
- **Intent** – Whether the agent intends harm
- **Limits** – Legal and ethical limits of agent
- **Outcome** – Purpose of attack / primary goal
- **Objective** – Method agent uses for *Outcome*
- **Resources** – Available time, money & technology
- **Skills** – Special training and expertise
- **Visibility** – How hidden are identity and actions

Building An Agent

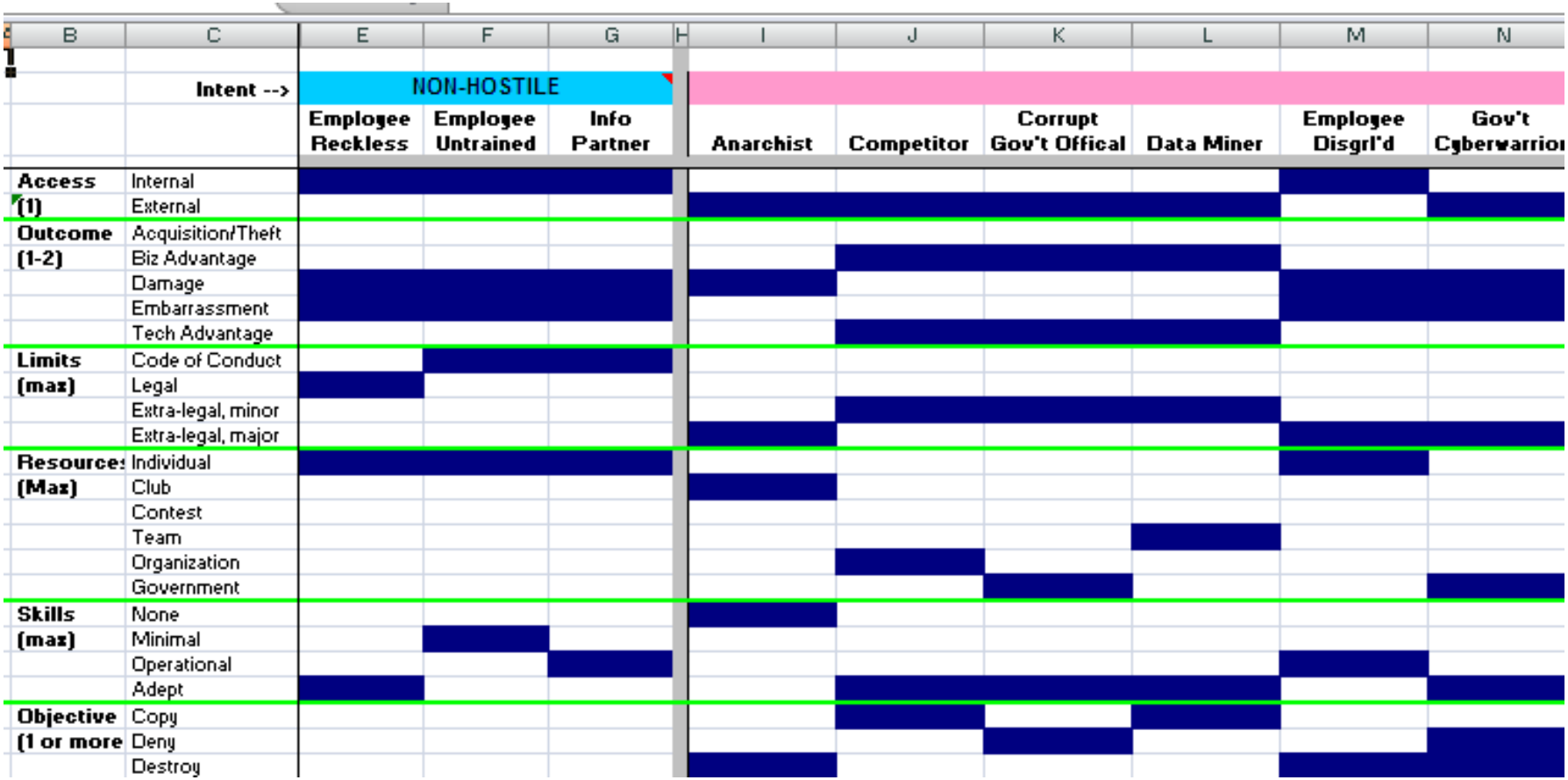
1. Start with a concept or prototype, e.g. “someone who mines open source info for company secrets”
2. Define what it is, and what it isn’t – this is often a very long process
3. Map the agent to the taxonomy
4. Refine the definition by iterating between #2 & #3
5. Research examples of the agent & activities to fill in the archetype
6. Assign the simple label, e.g. “Data Miner”

This process highlighted the enormous complexity behind simple labels like “hacker,” and greatly improved our understanding of the attackers, their methods, and highest threats

Agent Descriptions

- Each agent has a unique attribute map
- Each agent also has a detailed text description, much like a software design “persona”
- Archetype of the agent created from the norm, not the outlier
  - Intent is to simplify threat analysis and eliminate noise
- Drawn from research and actual case studies where available

Excerpt: Agents-Attributes Map



		Intent -->	NON-HOSTILE								
		Employee Reckless	Employee Untrained	Info Partner	Anarchist	Competitor	Corrupt Gov't Offical	Data Miner	Employee Disgrl'd	Gov't Cyberwarrior
Access	Internal	■	■	■					■	
(1)	External				■	■	■	■		■
Outcome	Acquisition/Theft									
(1-2)	Biz Advantage					■	■	■		
	Damage	■	■	■	■				■	■
	Embarrassment	■	■	■					■	■
	Tech Advantage					■	■	■		
Limits	Code of Conduct		■	■						
(max)	Legal	■								
	Extra-legal, minor					■	■	■		
	Extra-legal, major				■				■	■
Resources	Individual	■	■	■					■	
(Max)	Club				■					
	Contest									
	Team							■		
	Organization					■				
	Government						■			■
Skills	None				■					
(max)	Minimal		■							
	Operational			■					■	
	Adept	■				■	■	■		■
Objective	Copy					■		■		
(1 or more	Deny						■			■
	Destroy				■				■	

Using the Library

- Regular threat reports
- Design assistance for product security
- Simplified risk assessments

Agent Activity & Threat Analysis

Example:

- **Espionage & Theft Threat Agents** continue to be driven by poor worldwide economy, sustaining IP theft threat at current high levels, placing IP at higher risk.

- **Cyberwar Forces** are receiving considerable press but there is little evidence that non-military high-tech *companies* in general are a primary target for an actual attack. High-tech *products*, however, are a key component of the world's IT infrastructure and are receiving increasing scrutiny from both attackers and regulators.

Example Threat Agent Trending – *Corporate-specific*

Agent	Recent Activity	Predicted Trend
Agent A		
Agent B		
Agent C		
Agent D		

Example Persona: *Reckless Employee*

Mary Jane
Factory Employee
12 years/Tech grade
Senior Floor Lead

Mary attended an offsite vendor class on a new version of a common manufacturing tool. While in class Mary had a heated discussion about how the tool can be used. She revealed a simple but undocumented use that skipped steps in the process, saving 3 days in processing time. Employees from competing companies were present in the class.

Mary's disclosure allowed the competitors to narrow the cost gap. Estimated loss: >$30M

Targeted Risk & Threat Assessment

For small domains or narrow targets

- Subject Matter Experts (SMEs) examine problem set and identify 2-4 “most likely” threat agents
- Assessment and design work focuses on those agents *only*
- Incorporated into Intel assessment tool (RAPLite)

Minimizing the number of agents reduces noise and streamlines the process, focusing the team on the greatest threats.

Domain-wide Risk & Threat Assessment

In large domains where all threats considered

- Subject Matter Experts build model (attack tree, etc.) to determine most likely avenues of attack
- Agents to most likely avenues then "summed," highlighting most common skill & resource levels
- This approach used by U.S. Dept. of Homeland Security for first national risk assessment (*IT Sector Risk Assessment [Baseline]*)

This method reduced one large Intel threat assessment from two months to 1 day.

Future Work

- Candidate new agents
  - "Embezzler" - employee abusing IT privileges for financial gain
  - "Internal Agitator" – employee seeking attention for personal cause by leaking sensitive information
- New methods
  - XML versions
  - Exploit matrix
  - Mathematical attribute sampling
  - Automated agents and gaming

The Library Developers

- Don Byrne
- Tim Casey
- Lonnie Hurst
- Greg Kime
- Toby Kohlenberg
- Daniel Lewis
- Steve Mancini
- Martin Martinez
- Wil Milan
- Kim Owen
- KC Rich
- Matt Rosenquist
- Keith Shippy
- David Ulmer
- Brian Willis
- Tom Weisser
- Calvin Wong

Questions?

Additional Resources

- IT@Intel Threat Agent Library white paper
  - http://communities.intel.com/docs/DOC-1151
- DHS IT Sector Risk Assessment (Baseline)
  - http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf
- IT@Intel Threat Agent Risk Assessment (TARA) Methodology white paper
  - www.intel.com/it
- RAPLite white paper

Additional Resources

- IT@Intel Threat Agent Library white paper
  - http://communities.intel.com/docs/DOC-1151
- DHS IT Sector Risk Assessment (Baseline)
  - http://www.dhs.gov/xlibrary/assets/nipp_it_baseline_risk_assessment.pdf
- IT@Intel Threat Agent Risk Assessment (TARA) Methodology white paper
  - www.intel.com/it
- RAPLite white paper
  - http://www.intel.com/it/pdf/aligning-business-and-information-risk-assessments.pdf

Intel Information Technology

Know Thy Enemy: *Cataloguing Agents of Threat for Improved Risk Assessments*

FIRST Conference, June 2010

Legal Notices