RSA CONFERENCE 2014
FEBRUARY 24 – 28 | MOSCONE CENTER | SAN FRANCISCO

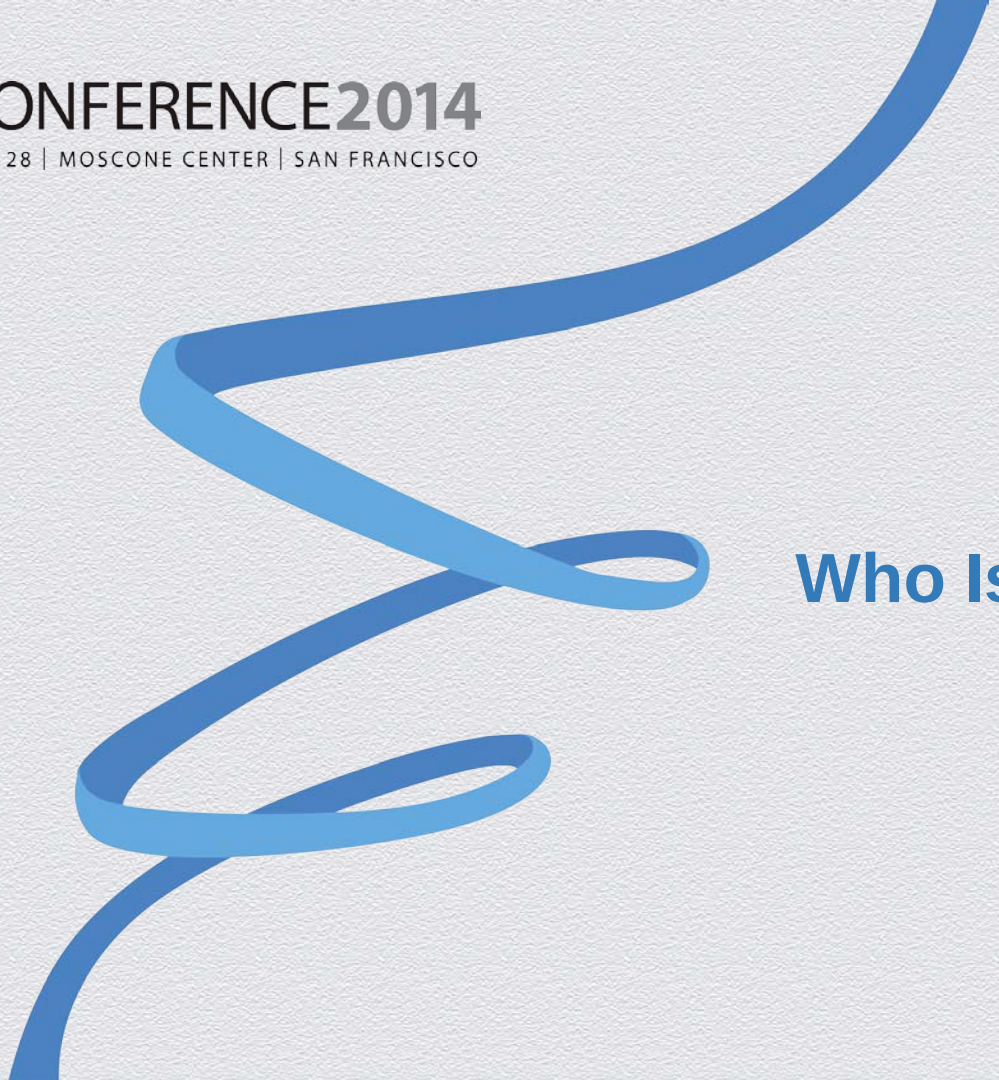
Share.
Learn.
Secure.
Capitalizing on
Collective Intelligence

Let Go of the Status Quo: Build an Effective Information Protection Program

SESSION ID: DSP-W01

Daniel Velez

Director, Insider Threat Operations
Raytheon Cyber Products Company
daniel.velez@raytheon.com
703.244.9887



Who Is Looking?

Sabotage

Image: www.navy.mil

UNITED STATES ATTORNEY'S OFFICE
EASTERN DISTRICT OF VIRGINIA

ALEXANDRIA NEWPORT NEWS NORFOLK RICHMOND

UNITED STATES ATTORNEY CHUCK ROSENBERG

FOR IMMEDIATE RELEASE:

April 5, 2007

Jim Rybicki
Public Information Officer
Phone: (703) 842-4050 Fax: (703) 549-5202
E-Mail: usavae.press@usdoj.gov
Website: www.usdoj.gov/usao/vae

Further Information Contact:
Deanna Warren
Phone: (757) 441-6331

Former Navy Contractor Sentenced for Damaging Navy Computer System

(Norfolk, Virginia) – Richard Sylvestre, 43, of Boylston, Massachusetts, was sentenced yesterday to 12 months and one day in prison, followed by three years of supervised release, and ordered to pay a $10,000 fine and $25,007 in restitution, upon his conviction for damaging protected United States Navy computers. Chuck Rosenberg, United States Attorney for the Eastern District of Virginia, made the announcement after Sylvestre was sentenced by United States District Judge Rebecca Beach Smith.

Raytheon

The Status Quo

Insider Threat

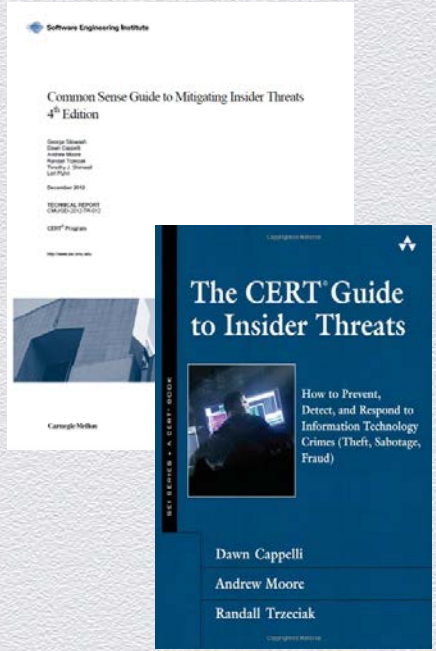
- Authorized access
- Causes harm
  - Fraud
  - Sabotage
  - Theft
  - Violence
  - Lack of knowledge
- Your information technology system is sometimes witness, victim, or enabler

Why Aren’t We Auditing?

- Our corporate culture
- Lack of resources
- It’s new for us, and it looks hard
- We haven’t been hit (yet)

It's Common Sense

- "log, monitor, and audit employee actions"
- "…additional auditing of sensitive files"
- "detect activities outside of the employee's normal scope of work"
- "audits of account creation and password changes by system administrators"



Inadequate auditing is an issue of concern

Raytheon

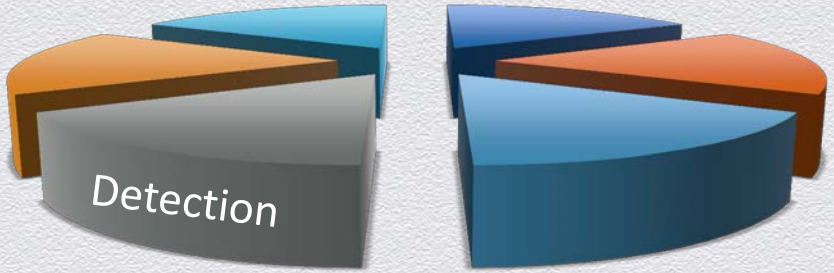
Getting What You Expect

"Don't expect what you don't inspect…"

The Success System That Never Fails (1962) by W. Clement Stone

Do you have the will to inspect?

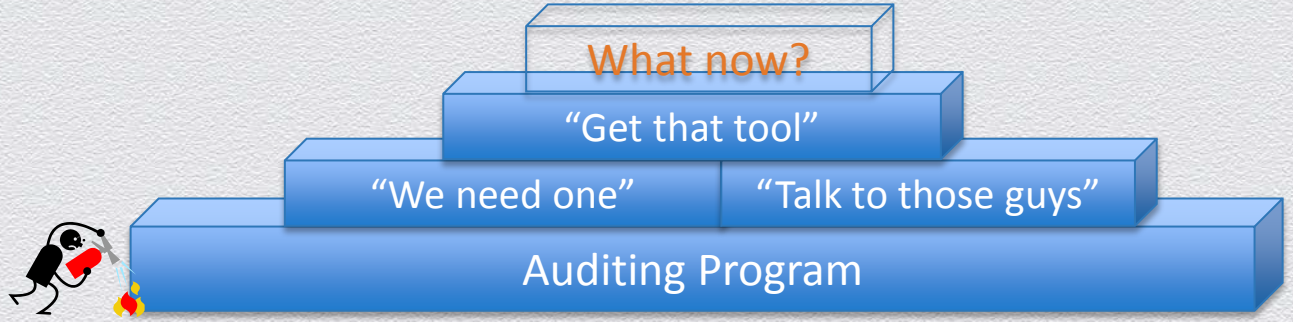
What Makes A Complete Insider Threat Program?



- Policies
- Processes
- Technical Controls
- Training & Awareness
- Risk Management
- Auditing & Monitoring

Prevention > Detection

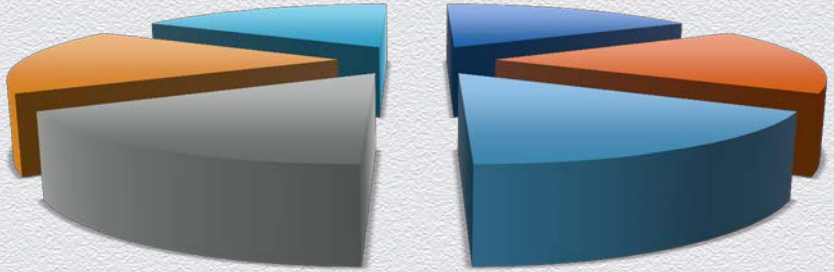
Catalyst for Identifying a Solution?



This is not just a technology problem

Raytheon

The Complete Insider Threat Program



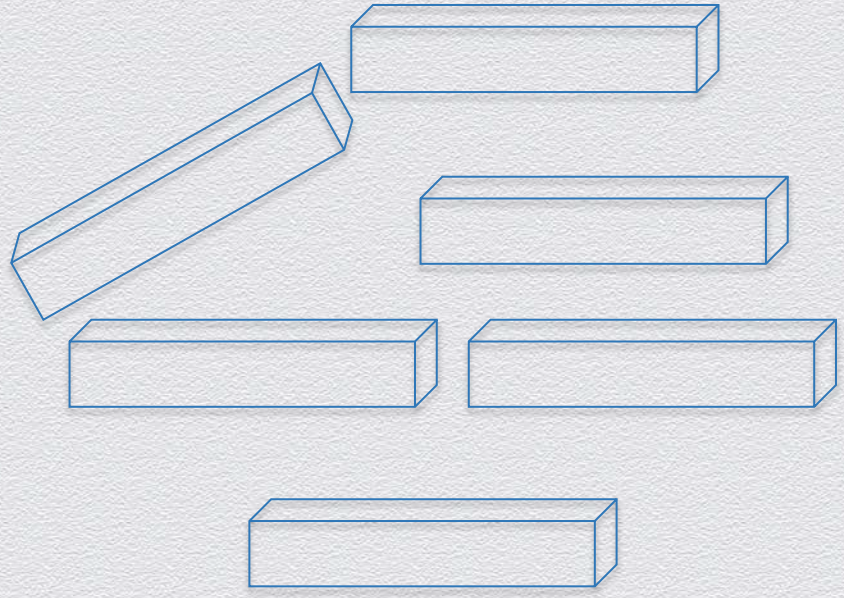
- Policies
- Processes
- Technical Controls
- Training & Awareness
- Risk Management
- Auditing & Monitoring

Technology's role: Support the program

A Solid Foundation

Must-Haves

1. Establish an Insider Threat Program
2. Business Case
3. Staff
4. Stakeholders
5. Education
6. Governance
7. Document the Activity
8. Tool Selection
9. Implementation

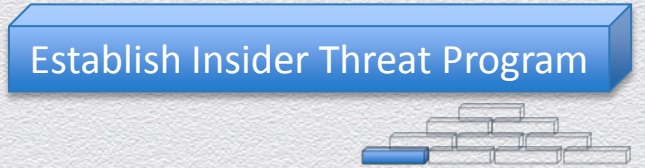


*Michael Theis
Carnegie Mellon

Hope is not a strategy*

Raytheon

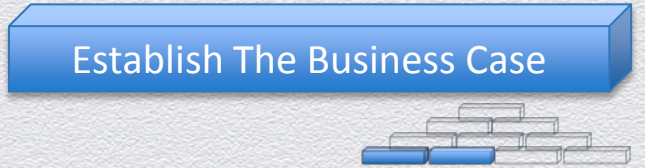
Establish A Program



- Top-down direction and advocacy
- Establish the vision
  - Gives the organization the will; reduces the feet dragging
- Put someone in charge
  - If you can't point at the person responsible when something goes wrong…
- Define roles and responsibilities: prevent, detect, respond

Priority 1: Start here

A Common Understanding



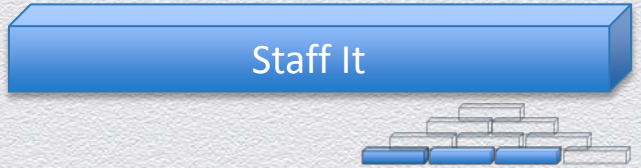
If you don't understand WHY you're implementing your auditing and monitoring program, then STOP.

- Authority, Directives, Instructions
- Risk assessment and validated requirements
- PCI Data Security Standards
- EO 13587
- FINRA Audit Trail requirements
- HIPAA Security Standards: Audit Controls

Map your auditing plan to your business case

Raytheon

Building The Staff



- Security fundamentals and their legal issues: laws, regulations, and best practices regarding the use of records and data
- Insider threat training
- Your procedures for prevention, detection, and response
- Proficient with forensics tools
- Desktop engineering
- Additional screening and vetting; non-disclosure agreements
- Policy authors

The quality of your staff is more important than the technology

Raytheon

Who Should Be Involved?

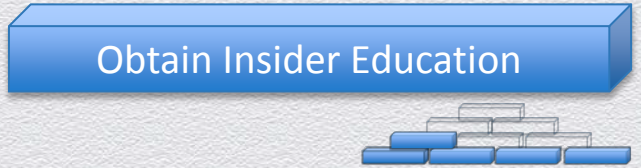
Engage Stakeholders Early

- Computer network defense
- Computer investigations
- Security
- Unions
- CIO
- HR
- LE/CI
- Counsel
- Internal audit

Identify your stakeholders and their requirements

Raytheon

There Is No Easy Button



Art

- History, war stories
- Creative auditing
- Current events and trends
- Risk management
- Stakeholders

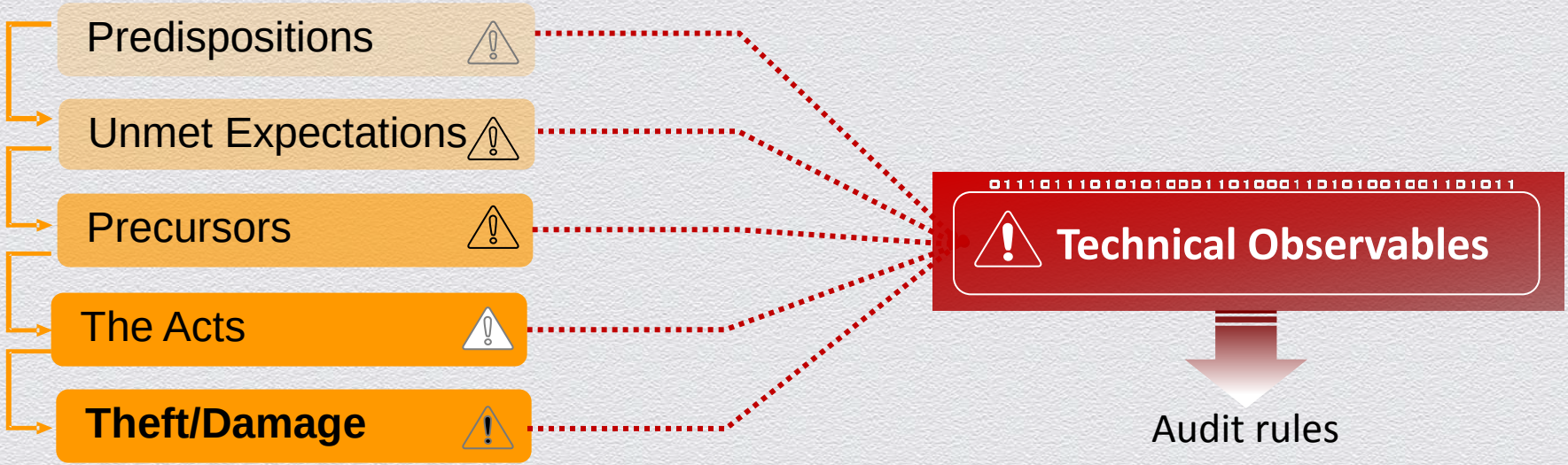
Science and Math

- Automated detection
- Deviation from baseline
- Alerts based upon algorithm
- Behavioral sciences
- Free from human biases

Finding Your Insider Threat

Obtain Insider Education

- SEI Insider Threat Workshop: http://www.cert.org/insider_threat/



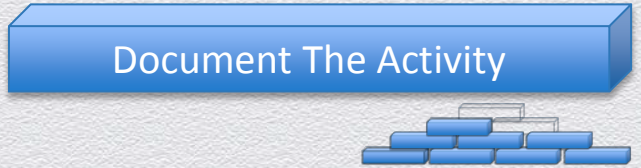
Understand *how* technology is an enabler

The Washington Post Test

- Engage your legal counsel
- Verifies you are operating per authority, policies
- Identify abuses in operation
- Initiation of inquiries, escalation
- Approve audit rules – “Policy Control Board”
- Access to audit records, content

No cowboys in the basement

Answer The Basic Questions



Document your principles, assumptions, requirements

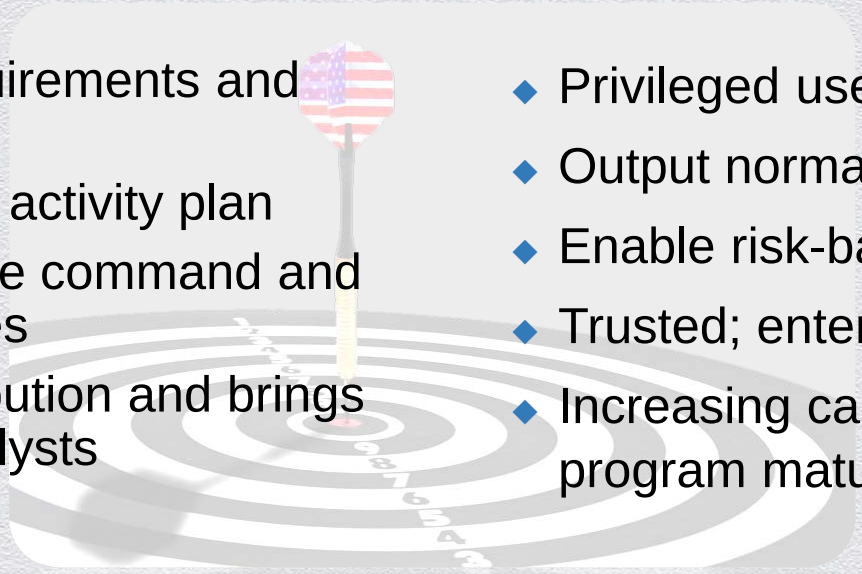
- Who
  - Data owner?
  - Deploys the tools?
  - Access to the data?
- What
  - Business case?
- When
  - Event, content, more
  - Release data?
- Where
  - Which networks, campus?
- How
  - Overt? Hidden?
  - Using enterprise IT?
- Why
  - Audits or inquiries?
  - Risk management interfaces?

Your team will need clear guidance

Raytheon

Tool Selection Tips

Select a Tool That Fits

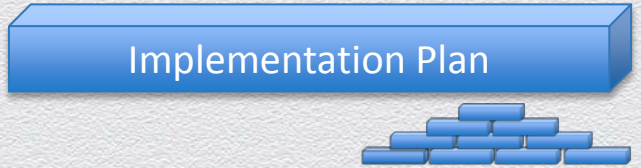


- Technical requirements and architecture
- Supports your activity plan
- Don’t forget the command and control features
- Provides attribution and brings context to analysts
- Privileged user-tough
- Output normalized for humans
- Enable risk-based approach
- Trusted; enterprise-ready
- Increasing capabilities as your program matures

Auditing should provide answers, not more questions

Raytheon

Defeating Obstacles



- Expect this IT project to require non-IT resources and energy
- Lab installation saves implementation time – ask for one
- Your vendor should provide an implementation plan – demand it
- Don’t forget a communications plan directed at your users – culture
- Ask your vendor about Help Desk tools and training
- The placebo effect – get ready for blame
- Plan to continuously improve audit policies – not set and forget

Ask your vendor to describe the best plans

Raytheon

You Will Be Better Prepared Than Most

- Establish Insider Threat Program
- Establish The Business Case
- Staff It
- Engage Stakeholders Early
- Obtain Insider Education
- Governance and Oversight
- Write a Concept of Operations
- Select a Tool That Fits
- Implementation Plan

Raytheon

What questions do you have?

Daniel Velez
Operations
Raytheon Cyber Products Company

703.244.9887
daniel.velez@raytheon.com
pgp 0x4E6EE322

Backup Slides