

Protecting Against and Investigating Insider Threats

*A methodical, multi-pronged approach
to protecting your organization*

Antonio A. Rucci

Program Director

Technical Intelligence and Security Programs

Global Initiatives Directorate

Oak Ridge National Laboratory

Oak Ridge, TN 37831





www.ornl.gov

AGENDA

*A methodical, multi-pronged approach
to protecting your organization*

- **Key indicators of an insider threat and how to detect them**
- **Specific hiring practices to minimize your risk**
- **Security awareness training and education to thwart opportunistic individuals**
- **Recent case studies that illustrate the key indicators and how to protect against them**



AGENDA

*A methodical, multi-pronged approach
to protecting your organization*

- **Key indicators of an insider threat and how to detect them**
- Specific hiring practices to minimize your risk
- Security awareness training and education to thwart opportunistic individuals
- Recent case studies that illustrate the key indicators and how to protect against them



Who Are The Insiders?

- **Employees**
- **Former Employees**
- **Contractors**
- **Consultants**
- **Suppliers**
- **Visitors**
- **Collaborators**
 - User facilities
 - University faculty
 - Industry





Pre-conditions

- **Motive** or need to be satisfied through the crime
- **Ability to Overcome Inhibitions:**
 - Moral values
 - Fear of being caught
 - Loyalty to employer or co-workers
 - Risk-Taking Behaviors
- **Trigger** that sets the betrayal in motion
- **Opportunity** to commit the crime
 - Poor and/or lax security practices



Motive

- **Financial**
- **Anger**
- **Excitement**
- **Divided loyalties**
- **Arrogance**
- **The BIG 3:**
 - **Greed**
 - **Disgruntlement**
 - **Revenge**





THE OATH

...solemnly swear that I will support and defend the Constitution of the United States...bear true faith and allegiance...will well and faithfully discharge the duties of the office...So help me God.

ESPIONAGE

The act of obtaining, delivering, transmitting, communicating, or receiving information about the national defense with an intent, or reason to believe, that the information may be used to the injury of the United States or to the advantage of any foreign nation.



Robert P. Hanssen
Spy • Traitor • Deceiver

Office of the National Counterintelligence Executive

www.ncix.gov



Ability to Overcome Inhibitions

- **Moral Values**
- **Ethical Values**
- **Loyalty**
- **Fear**
- **Rationalization**



Trigger

- **Personal or professional event**
- **Stress pushes individual to the “breaking point”**
 - React negatively, and criminally
 - Emotionally stable/well adjusted
 - React to stress in a positive manner



At least 1/4 of American spies experienced a personal life crisis in the months preceding an espionage attempt.

— | A Study CONDUCTED BY THE VERIZON BUSINESS RISK TEAM | —

2008 DATA BREACH INVESTIGATIONS REPORT

Four Years of Forensic Research. More than 500 Cases.
One Comprehensive Report





ArcSight ~~X~~ *Top 10 Insider Threats*

- 1. Proving that the Vendor's Insider Threat Claims are Valid**
- 2. Converging Insider Threat with Physical Security**
- 3. Demanding ROI and ROSI for your Insider Threat Program**
- 4. Converging IT Threat with IT Governance & Regulatory Compliance**
- 5. Understanding that Insiders are People too**
- 6. Leveraging Real-Time and Forensics Analysis to Pinpoint Insiders**
- 7. Providing Intelligent, Insider-Aware Response Capabilities**
- 8. Managing the Insider Threat**
- 9. Detecting the Insider Threat**
- 10. Insider Threats are Different than External Threats**



USSS & Carnegie Mellon University Survey Findings

- Most insider events were triggered by a negative event in the workplace
- Most perpetrators had prior disciplinary issues
- Most insider events were planned in advance
- Only **17%** of the insider events studied involved individuals with root access
- **87%** of the attacks used very simple user commands that didn't require any advanced knowledge
- **30%** of the incidents took place at the insider's home using remote access to the organization's network

**Developments in information technology
make it much harder to control the
distribution of information.**




**Items like these greatly increase opportunities for espionage and the
amount of damage that can be done by a single insider.**

**Developments in information technology
make it much harder to control the
distribution of information.**



Items like these greatly increase opportunities for espionage and the amount of damage that can be done by a single insider.

 nvidia 7800 wont work

i bought one of these and tried putting in my dell dimension 2350. my friend said that the shiny metal part on the bottom looks like it has lines because you cut at the lines if it doesnt fit. so i carefully cut off the bottom so that it fit into 1 of the slot things in my computer. now it doesnt work. did i cut it wrong? id post pics, but no camera. is there anyway i can fix this? thanks for any help.



EPIC FAILURES

Retardation is No Excuse for \$600 Mistakes



www.ornl.gov

AGENDA

*A methodical, multi-pronged approach
to protecting your organization*

- Key indicators of an insider threat and how to detect them
- **Specific hiring practices to minimize your risk**
- Security awareness training and education to thwart opportunistic individuals
- Recent case studies that illustrate the key indicators and how to protect against them



5 Simple Measures to Protect Your Organization from Insider Threats

- 1. Conduct Background Checks on all new employees**
- 2. Monitor employee behavior**
- 3. Restrict accounts that have remote access**
- 4. Restrict the scope of remote access**
- 5. Enforce the principle of “Least User Privilege”**



Screen Your Personnel

- **Initial Counterintelligence Screening & Periodic Reviews**
- **Financial records check**
- **IRS disclosure**
- **Records checks**



Contributing Factors

**Behavioral & Suitability
Issues**

**Socio-Economic
Factors**

**Psychological
Factors**

**Technological
Trends**



Behavioral Factors & Suitability Issues

- **Substance Abuse or Dependence**
- **Hostile, Vindictive, or Criminal Behavior**
- **Extreme, Persistent Interpersonal Difficulties**
- **Unreported Foreign Interaction**
- **Excessive Gambling / spending**
- **Internet presence... most will**

“Most known American spies (80%) demonstrated one or more conditions or behaviors of security concern” before they turned to espionage.”

Defense Personnel Security Research Center (PERSEREC) Report 2002



Socio-Economic Factors

- **Global Market is Expanding**
- **Increased Foreign Interaction**
- **Vulnerabilities (financial crisis)**
- **Organizational Loyalty is Diminishing**
- **Ethnic ties**
- **Moral Justification**



Psychological Factors

The Narcissist:

- Preoccupation with self at expense of others
- Grandiose sense of their own importance
- Exaggerate accomplishments
- Unjust victims of rivals
- Sense of entitlement

The Sociopath:

- Lack of conscience or morals
- Violates others rights to serve own means





What Can You Do?

- **Be alert**
- **Don't be paranoid, but report concerns**
- **Be aware of espionage indicators**
- **Screen your personnel**
- **Assess your personal vulnerabilities**



Rogue Warriors?

- **Appearing intoxicated at work**
- **Sleeping at the desk**
- **Unexplained, repeated absences on Monday or Friday**
- **Actual or threatened use of force or violence**
- **Pattern of disregard for rules and regulations**
- **Spouse or child abuse or neglect**
- **Attempts to enlist others in illegal or questionable activity**
- **Drug abuse**
- **Pattern of significant change from past behavior, especially relating to increased nervousness or anxiety, unexplained depression, hyperactivity, decline in performance or work habits, deterioration of personal hygiene, increased friction in relationships with co-workers, isolating oneself by rejecting any social interaction**
- **Expression of bizarre thoughts, perceptions, or expectations**
- **Pattern of lying and deception of co-workers or supervisors**
- **Talk of or attempt to harm oneself**
- **Argumentative or insulting behavior toward work associates or family to the extent that this has generated workplace discussion or has disrupted the workplace environment**
- **Writing bad checks**
- **Failure to make child support payments**
- **Attempting to circumvent or defeat security or auditing systems, without prior authorization from the system administrator, other than as part of a legitimate system testing or security research**

Regardless of the technology in place to protect data, people still represent the biggest threat

Alex Ryskin





www.ornl.gov

AGENDA

*A methodical, multi-pronged approach
to protecting your organization*

- Key indicators of an insider threat and how to detect them
- Specific hiring practices to minimize your risk
- **Security awareness training and education to thwart opportunistic individuals**
- Recent case studies that illustrate the key indicators and how to protect against them

**OAK RIDGE
OFFICE
OF
COUNTERINTELLIGENCE**



is sponsoring the following FREE Seminar at the
Oak Ridge National Laboratory

Please contact Polly Bryson at 241-0646
if you are interested in attending

Wednesday, August 6, 2008

1:00 - 3:00 pm

Building 5100, Room 128, JICS Lecture Hall

***Anatomy of an Insider Threat:
Case Study in Human
Vulnerabilities***

The world's leading news organizations are reporting on the growing number of insider threats at work. These threats are not just a matter of lost productivity and lost revenue, but also a matter of national security. This seminar will explore the anatomy of an insider threat, from the initial vulnerability to the final act of betrayal. The seminar will be presented by two leading experts in the field of insider threats, Don Fingleton and Rich Sullivan. The seminar is free and open to all employees of the Oak Ridge National Laboratory. For more information, please contact Polly Bryson at 241-0646.

The seminar will be presented by two leading experts in the field of insider threats, Don Fingleton and Rich Sullivan. The seminar is free and open to all employees of the Oak Ridge National Laboratory. For more information, please contact Polly Bryson at 241-0646.

The seminar will be presented by two leading experts in the field of insider threats, Don Fingleton and Rich Sullivan. The seminar is free and open to all employees of the Oak Ridge National Laboratory. For more information, please contact Polly Bryson at 241-0646.

Instructors - Don Fingleton and Rich Sullivan

Take Advantage of Training Opportunities

Seek Out Training Opportunities

Create Unique & Innovative Training



Make Training Interesting

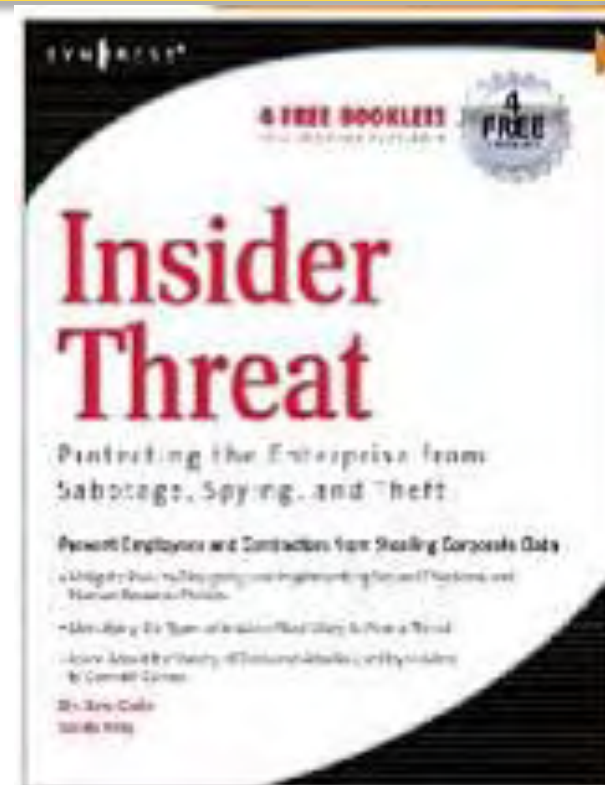
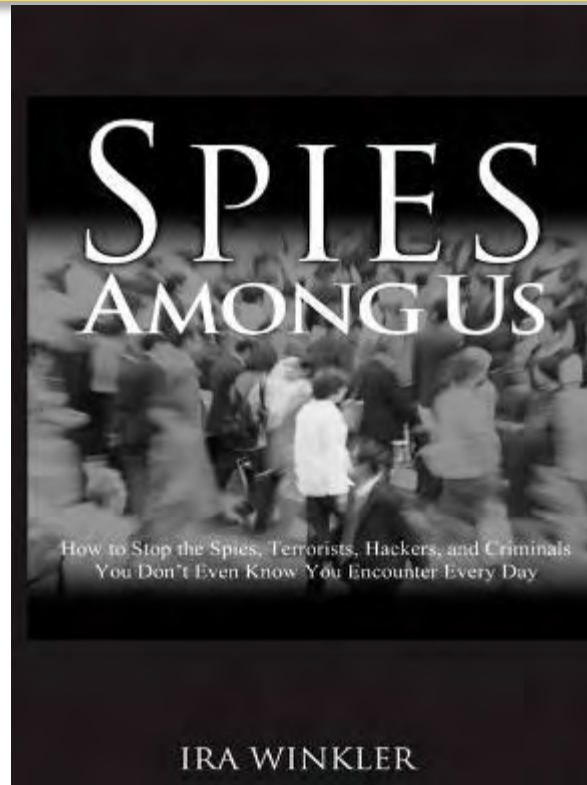
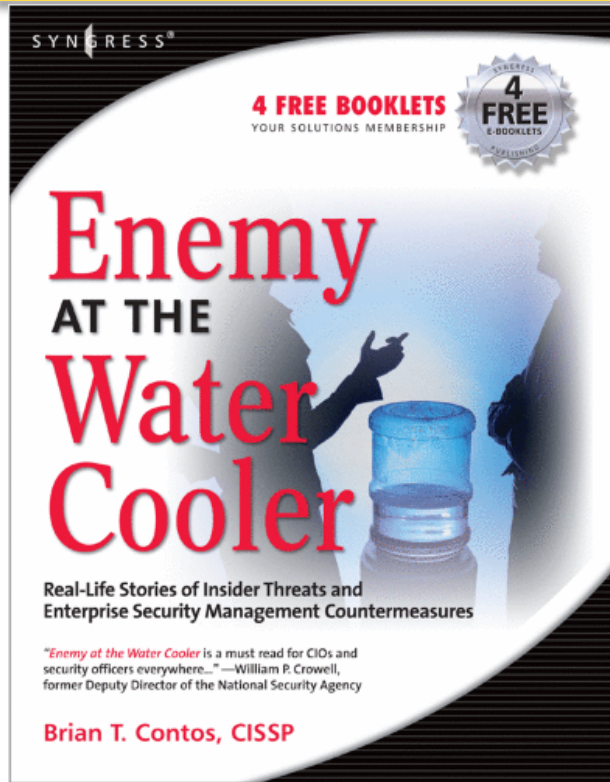


- **Bring external experts to your organization**
- **Make your training relevant, interesting and FUN!**
- **Case Studies are excellent training platforms**





Relevant Reading



www.cicentre.com



www.ornl.gov

AGENDA

*A methodical, multi-pronged approach
to protecting your organization*

- Key indicators of an insider threat and how to detect them
- Specific hiring practices to minimize your risk
- Security awareness training and education to thwart opportunistic individuals
- **Recent case studies that illustrate the key indicators and how to protect against them**

We need to build security into the core fabric, the DNA of the computing world.

Howard Schmidt



Case Studies



0100110001101001 0111010001100101 0101001101110100 0110111
0111001001101101 00100000 01010100 01100101 01100011 01101000
01101110 01101111 01101100 01101111 01100111 01101001 01100101



We must inspire a commitment to security
rather than merely describing it.

Mich Kabay





The brave new world of IPv6

01010100 01101000 01100001
01101110 01101011 00100000
01011001 01101111 01110101

Antonio A. Rucci

rucciaa@ornl.gov

www.twitter.com/InsiderThreats



www.ornl.gov

0100000101101100011011000010000001111001011011110111010101
1100100010000001100010011010010110111001100001011100100111
1001001000000110000101110010011001010010000001100010011001
0101101100011011110110111001100111001000000111010001101111
00100000011101010111001100100001