

**From  
Raxacoricofallapatorius  
With Love**

**Case Studies in Insider Threat**

# AGENDA

- Introduction & Curriculum Vitae
- History & Current Events
- Definitions
- Case Studies
- Current Research
- Sources





**FAMOUS  
(Infamous?)  
INSIDER  
THREATS**

Cost to pay Insider Dr. Ten Hong Lee to turn over highly sensitive and valuable proprietary manufacturing information and research data:

**\$150-160k**



Ability to leap frog years of experimentation and bring a product similar to Avery's to market immediately: **PRICELESS!**





**I give it out to six people, and if I can't trust them to that degree, then I have no desire to make it.**



## **Industrial Espionage VS Economic Espionage**

# INDUSTRIAL ESPIONAGE

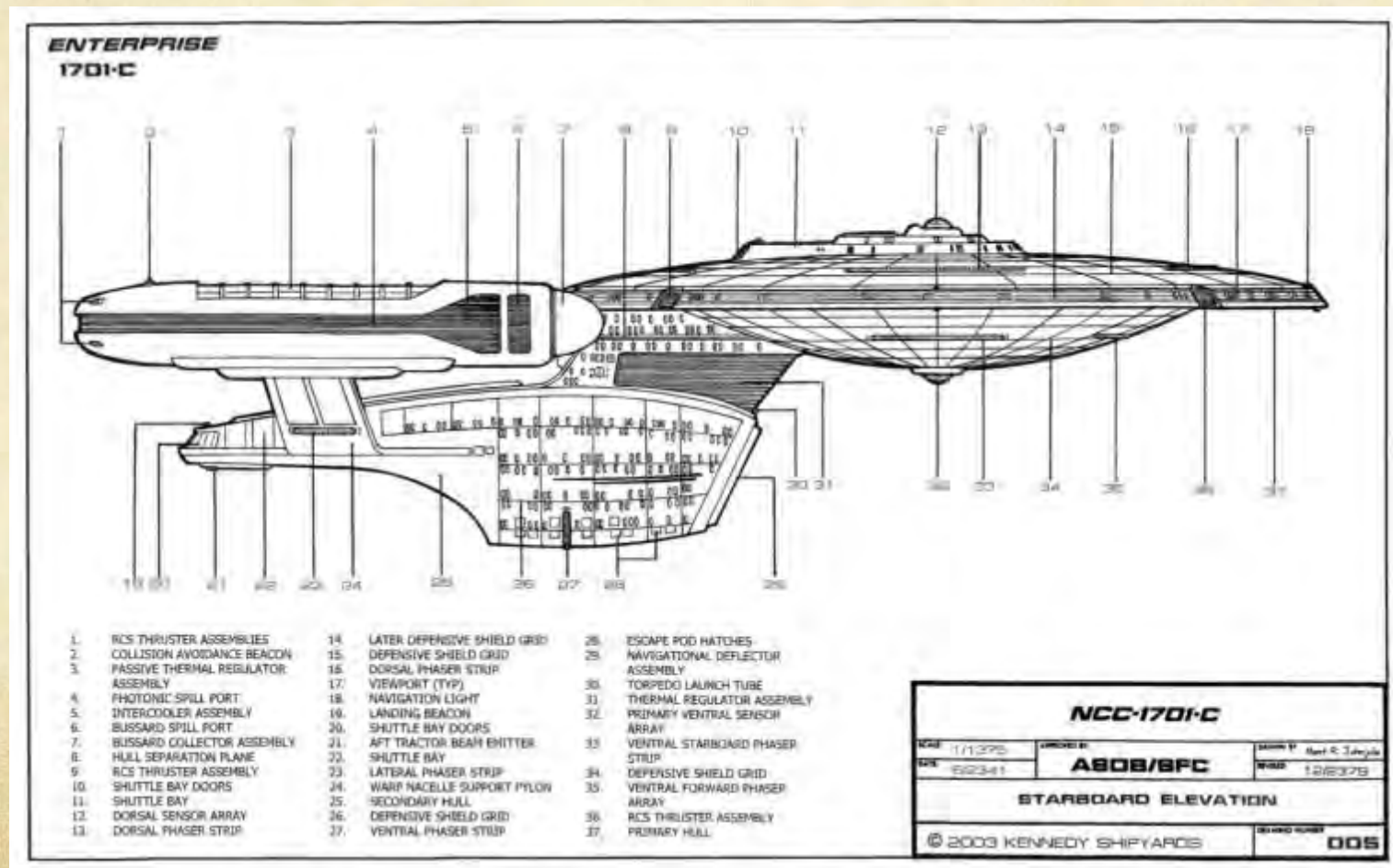
The theft of trade secrets by the removal, copying or recording of confidential or valuable information in a company for use **by a competitor.**



# ECONOMIC ESPIONAGE

The targeting or acquisition of trade secrets to knowingly benefit any foreign government, foreign instrumentality, or foreign agent.

(Title 18 U.S.C., Section 1831)





# SPY

A pre-existing trust or relationship is not required (but can exist).

# TRAITOR

An established confidence that is betrayed.

# INSIDER THREAT

Can be willful or a result of ignorance/neglect. Is not always malicious in nature.





## **“Formal” Definition**

### **MALICIOUS Insider**

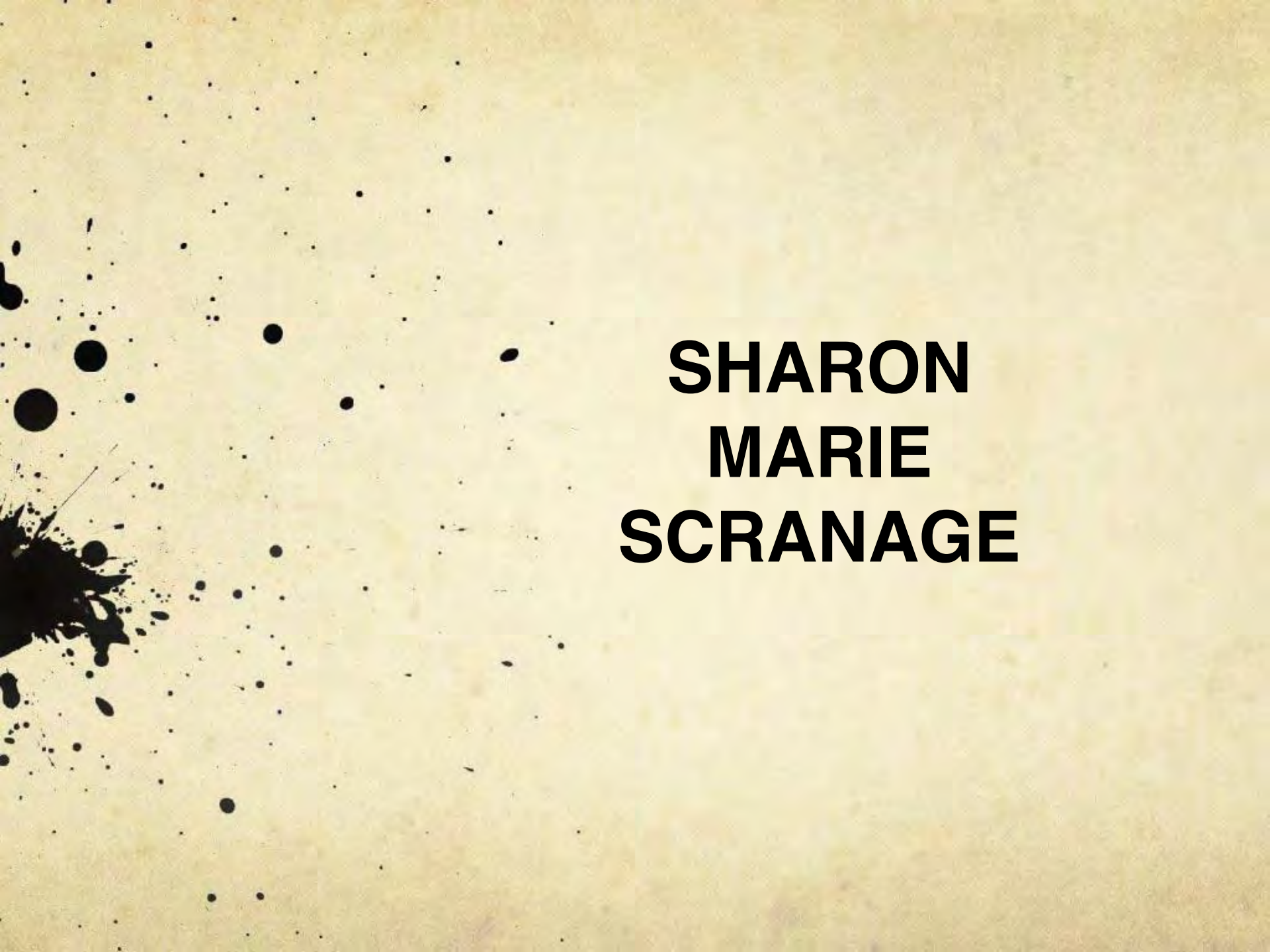
1. Current or former **employee, contractor, or business partner**
2. Has or had **authorized access**
3. **Intentionally exceeded or misused that access**
4. Negatively **affected the organization**



# hon·ey·pot

(ˈhənē,pät)

Espionage  
recruitment involving  
sexual seduction.



**SHARON  
MARIE  
SCRANAGE**

# Female CIA Employee compromised by male “honey pot”

**When?** 1980s (1983 -1985)

**Where?** Accra, Ghana

- Romance that evolved into threats of violence
- Information was stolen from files and cables
- Copied short hand and translated into long hand

## **RED FLAGS**

- Lover was cousin of Ghana President
- Lied about ending the relationship with him

## **Why was this case was important?**

- Intelligence Identities Protection Act
- Polygraph use helped break case



# GHANA



**1867**

English established control and created the British Gold Coast



**1966 – 1981**

Series of alternating military and civilian governments

**13<sup>th</sup> Century**

Several states created based on gold trading



**1957**

Coastal Gold Coast Region declares independence from the UK and establishes the nation of Ghana.



**1981**

Coup. Power seized by Flight Lieutenant **Jerry John Rawlings** of the Provisional National Defense Council. He suspended the constitution and banned political parties.



*Honour Student*

## **Leader of High School Cheerleading Squad**

*“Her hobby was going to church. That’s all she ever did.  
She had to be coerced.”*

*- Sharon’s brother, Perry Scranage*

**“...very religious type. Sang in the Baptist choir and could serve  
as a role model for any young girl.”**

**-Former High School Boyfriend, Richard Fortune**

*“....highly religious, never been in trouble...”*

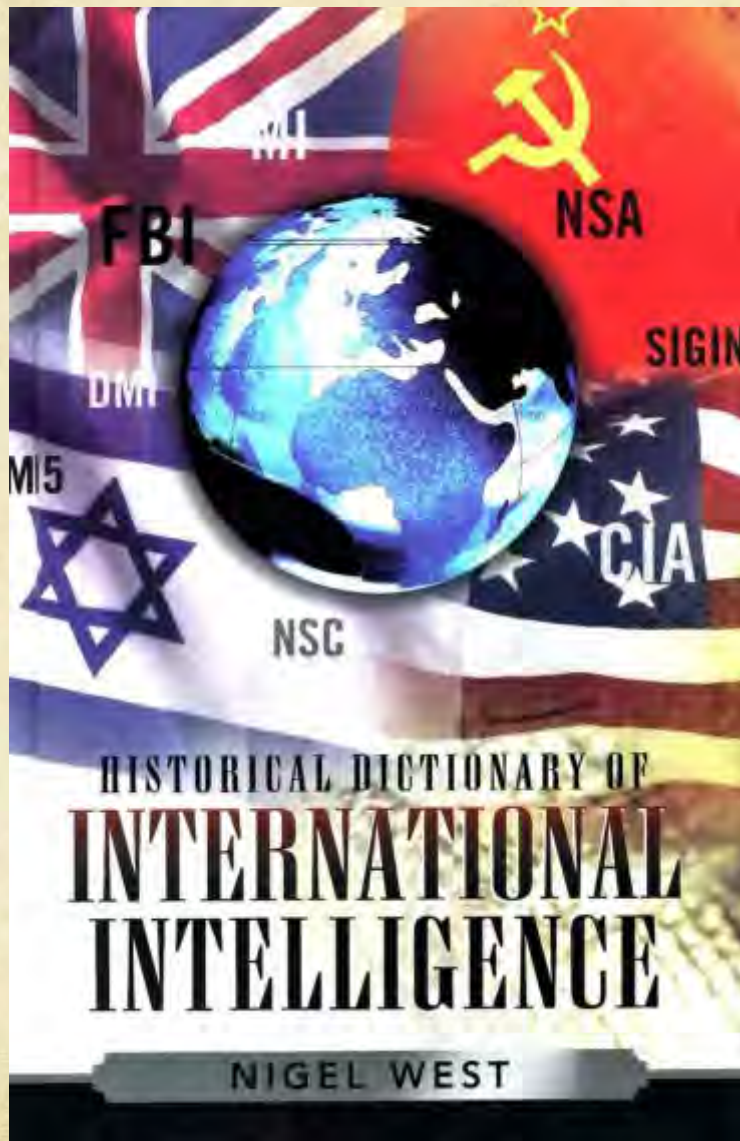
*-Friends and Family*

**“Shy naïve country girl who had never been overseas.”**

**-CIA Documents**







“Mousey young divorceé...

...recovering from an unhappy marriage...

...physically abused by ex-husband...

...isolated socially in the male dominated, largely white CIA station...

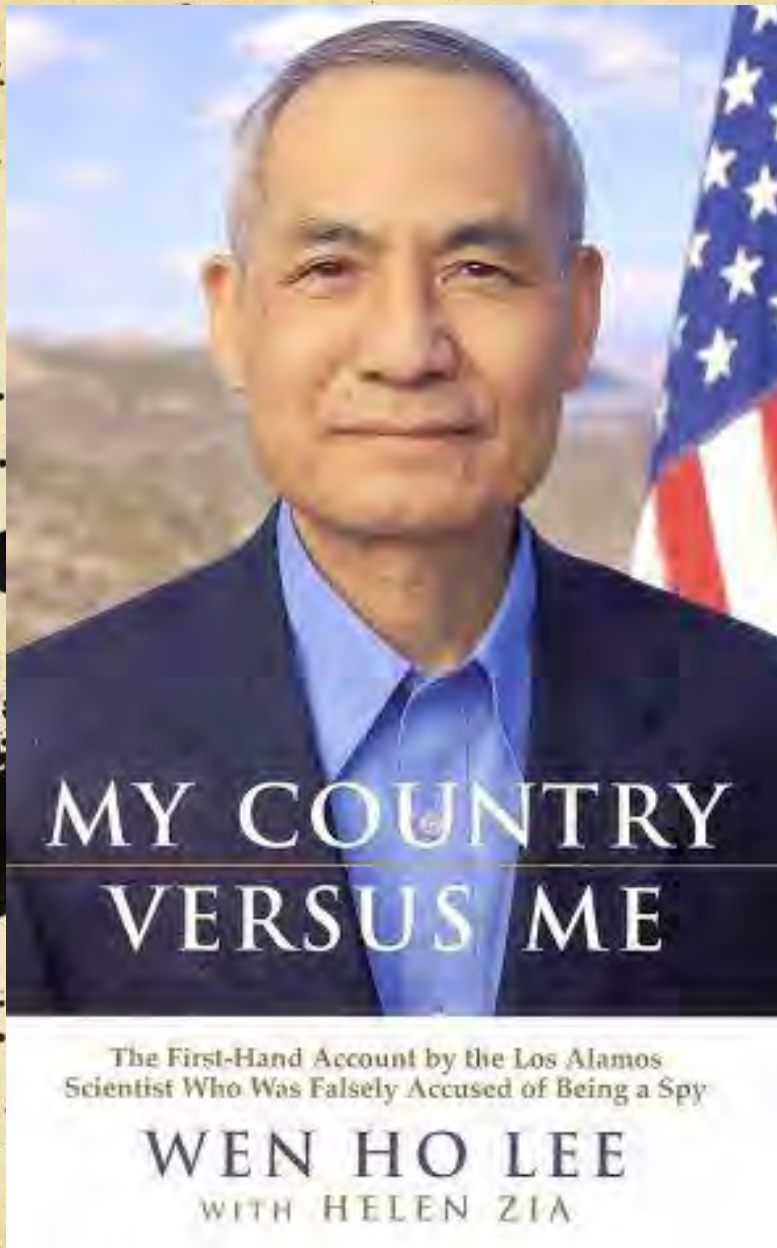
...Soussoudis could have been cultivating Scranage for further access at her next post in Calcutta...”



**I Am Not  
A Crook!**



**WEN  
HO  
LEE**



- 1939 Born in Nantou City, Taiwan  
Graduated Keelung High School
- 1963 Bachelors of Science in Mechanical Engineering from National Cheng Kung University in Tainan
- 1965 Came to the United States to study at Texas A&M
- 1969 Doctorate in Mechanical Engineering with Specialization in Fluid Mechanics
- 1974 Became a United States Citizen
- 1978-1999 Scientist in Weapons Design at Los Alamos National Laboratory in Applied Mathematics and Fluid Dynamics

# Indicted for stealing secrets on the US Nuclear Arsenal Insists he was not a spy. Accuses the government of abuse of power

**When?** 1978 – 1999  
**Where?** Los Alamos National Lab

- Downloaded restricted data
- Backed up work files
- Got access to system via a colleague after his access was denied



## RED FLAGS

- Lying about wiretap conversation
- Did not report attempt by foreign national to solicit classified by Dr. Side at hotel meeting
- Went through a work colleague to get access to data **AFTER** he had been denied and stripped of clearance
- Transferring that data to a third unclassified system

**Why this case was important?**

**Was he an insider threat?**



**US's  
First  
Economic  
Espionage  
Trial**



**DONGFAN**  
**“Greg”**  
**CHUNG**



# Stealing sensitive information on the U.S. space program with the intent of passing it to China

**When?** 1973 – 2006  
**Where?** California and Kansas

- Stored 300,000 pages of sensitive papers in his Southern California home.
- Prosecutors alleged the papers included information about the U.S. space shuttle, a booster rocket and military troop transports.
- Placed documents inside newspapers to take home at night.

## RED FLAGS

- Discovered while investigating Chi Mak
- Lied about “exchange scholar” Mr. Gu
- Trips to China

## Why was this case was important?

- US’s first economic espionage trial
- 1996 Economic Espionage Act





*Rose Palmisano, THE ORANGE COUNTY REGISTER*

## **Over 300,000 Sensitive Documents Seized From His Southern California Home to Include:**

- 24 Manuals on the B-1 Bomber
- Design Stress Analysis Manual on the Orbitor Vehicle 102
- Fighter Jet Structural Design Manuals
- F-15 Manufacturing Process Standards

## **SPACE SHUTTLE DOCUMENTS**

- Detailed Structure Diagrams
- Export Controlled Parts List
- Tutorial Marked With Export Restrictions
- 700 Documents related to the Shuttle Drawing System (SDS)
- Document on the Space Shuttle Hatch
- Space Shuttle Program Thermodynamic Design Data Book on the Thermal Control System

# THE SPY WHO COULDN'T SPELL





**BRIAN  
PATRICK  
REGAN**

# Convicted of offering to sell secret information to foreign governments

**When?** 1995 – 2000  
**Where?** Chantilly, Virginia

- Was in deep debt (\$117,000) and needed money
- Downloaded data & stole pages, CDROMs and video from NRO.
- Arrested at Dulles Airport with encrypted notes
- Buried classified material in the woods
- Used GPS; roofing nails hammered into trees; and complexly encrypted notes on the locations of the buried documents to find them again

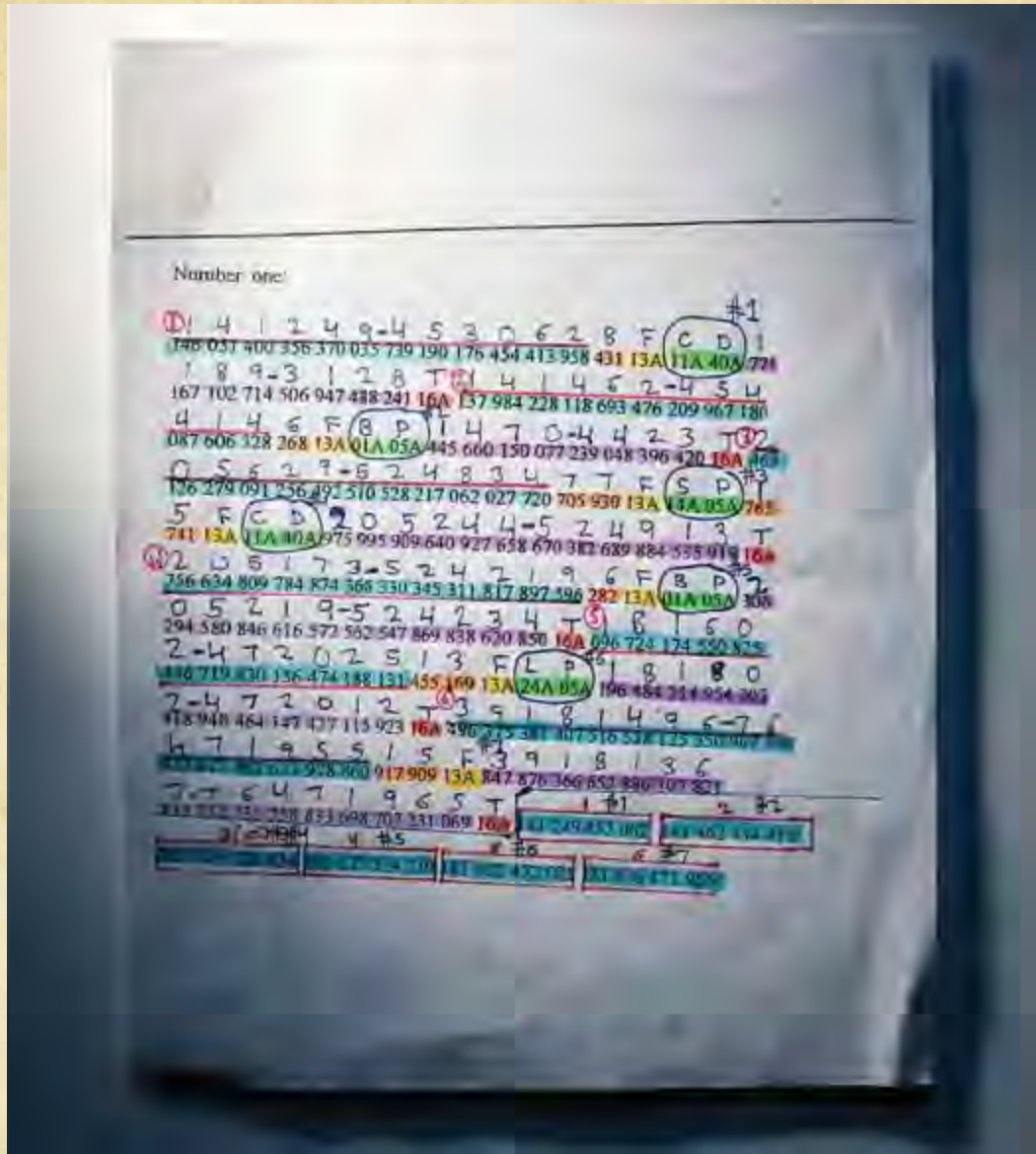
## RED FLAGS

- Financial Issues
  - \$117,000 in debt
  - Needed to send four kids to college

## Why this case was important?

Prosecutors sought the death penalty for the first time since the Rosenbergs in 1953.





**Brian Regan used a complex encryption scheme (left) to describe the locations of documents buried in a state park near Washington, DC (right).**

*Photo: Henrik Knudsen*

**Along with classified documents and contact information, he was carrying**

Folder containing 4 pages filled with three digit numbers (trinomes) 952, 832, 041...

**Found in right shoe:**

Contact information for the Iraqi, Libyan, and Chinese embassies in Switzerland

**Found in right trouser pocket:**

Spiral pad containing 13 seemingly unconnected words like tricycle, rocket, and glove

26 Words on an index card

**Found in his wallet:**

Piece of paper with a string of several dozen letters and numbers beginning 5-6-N-V-O-A-I...

**Along with classified documents and contact information, he was carrying**

Folder containing 4 pages filled with three digit numbers (trinomes) 952, 832, 041...  
**= encrypted latitude & longitude for the Virginia sites he buried his caches (based on an NRO phone list...used his junior high school year book for the Maryland sites)**

**Found in right trouser pocket:**

Spiral pad containing 13 seemingly unconnected words like tricycle, rocket, and glove **= Chinese missile sites**

26 Words on an index card **= Iraqi surface to air missile sites**

**Found in his wallet:**

Piece of paper with a string of several dozen letters and numbers beginning 5-6-N-V-O-A-I...  
**= a Caesar cipher revealing the addresses of several Swiss bank accounts**



**Found on a Post It note in his wallet:**

**hand, tree, hand, car**

**hand, tree, hand, car**



**hand, tree, hand, car**



**5**

**1**

**5**

**4**

# tricycle, rocket, glove



**3**



**1**



**5**

**Latitude Of Chinese Missile Sites**



# Current Research

# OVERVIEW of 5 CRITICAL PATHWAY COMPONENTS

Symantec White Paper

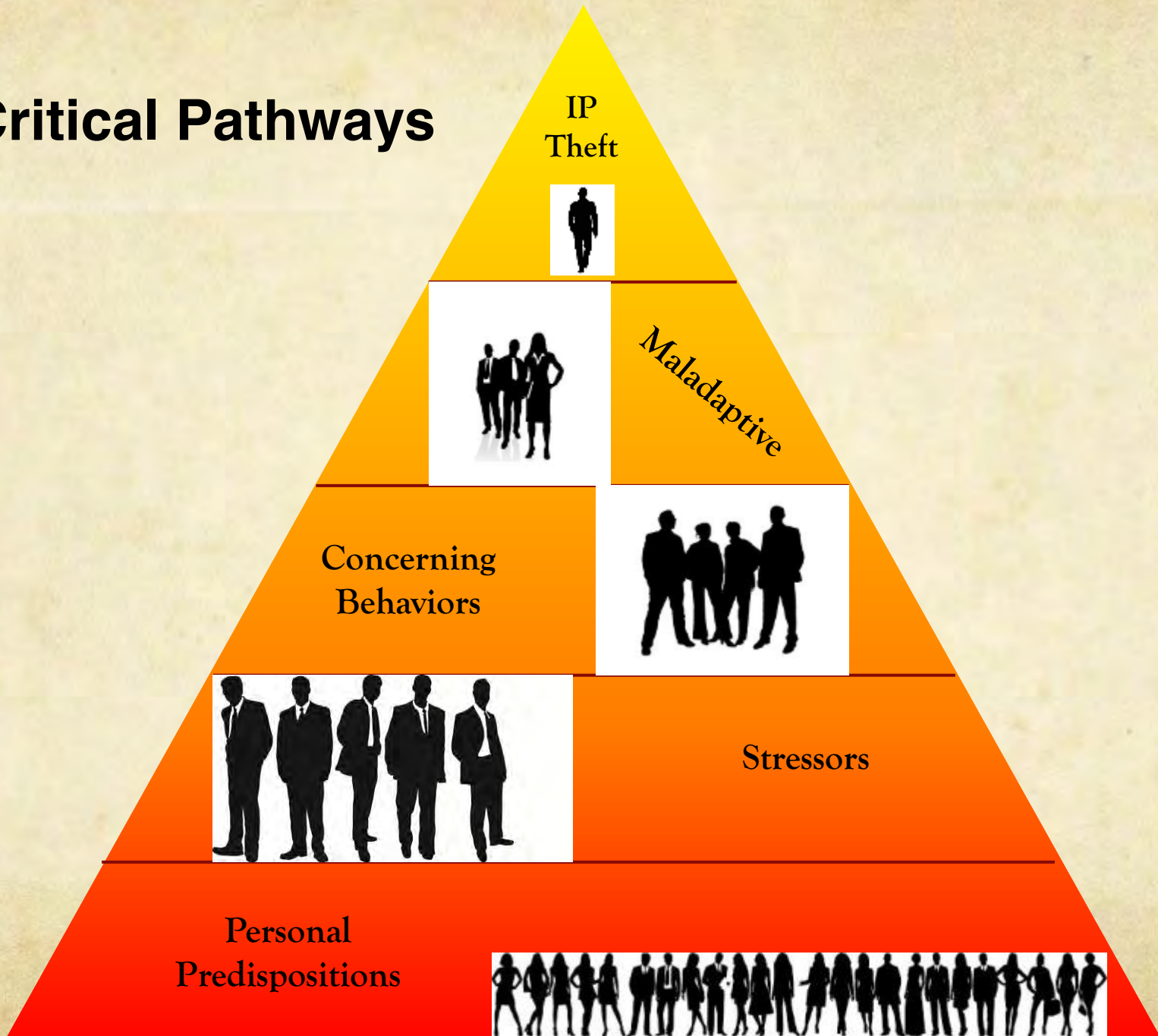
## Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall

*Eric D. Shaw, Ph.D. and Harley V. Stock, Ph.D., ABPP, Diplomate, American Board of Forensic Psychology*

1. Personal Predispositions in Individuals Vulnerable to Insider Risk Present **Prior to Joining** the Organization
2. **Personal** Stressors Noted in Subjects At-Risk for Insider Acts
3. **Professional** Stressors Noted in Subjects At-Risk for Insider Acts
4. **Concerning Behaviors or Violations of Policy, Practices or Law** Observed in Subjects At-Risk for Insider Acts
5. **Maladaptive Organizational Responses** to Subject Concerning Behaviors



# 5 Critical Pathways



# Identifying Personality Disorders that are Security Risks: Field Test Results

Olga G. Shechter  
Northrop Grumman Technical Services

Eric L. Lang  
Defense Personnel Security Research Center



**Antisocial Personality  
Disorder/Psychopathy**



**Narcissistic  
Personality Disorder**



# Insider Threat Control: Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time

Todd Lewellen  
George J. Silowash  
Daniel Costa

13 OCT 2013



**2** A **mosque** is a place of worship for followers of Islam and it is a House of prayer in Islam. **1** The Arabic name *masjid* is often used by Muslims which literally means place of prostration. A mosque is very important to Muslims because it is a way for man to recreate pure divine presence on earth.

**2** In English the word "mosque" refers to all types of buildings which are used for Islamic worship. There is no real pattern to build a mosque except on some few points. The direction of Mecca, qibla (kible), needs to have a clear indication in **3** a mosque. The orientation was more important than of for **3**. Mostly they have a mihrab, a **niche** in the wall. In front of the mihrab a mosque needs to have a roofed area.

In the smaller mosques five prayers daily are held, led by the Imam. In the larger mosques additional congregation sermons are held. These sermons are attended by **2** re people for example the Koran is taught there. A mosque is not only for praying, it is a **center** for education, information, and dispute settlement.

**1** Mecca is the first mosque, meaning the **3** a that surrounded the Kaaba. The Kaaba is the most holy shrine in the Islamic religion. The courtyard **6** of Muhammed's house in Madina was the model of e **5** y mosques. It was a mix of religious, social, political, and judicial functions. The qibla was first facing in the direction of Jerusalem and 1,5 years it faced Mecca.

**3** Mosques soon became mo **3** complex, and uniform. They have changed important from the open-air spaces. Th **1** got a minbar, where the Friday prayer is held. Mosques became such important **1** mbols within few years after the death of Muhammad. Islamic conquerors put up a mosque first, and then the military camp was built around it.

## Primary Source View

<b>1</b>	www.1011.com Internet source	26%
<b>2</b>	Submitted by Student P Student paper	8%
<b>3</b>	Submitted by Student P Student paper	5%
<b>4</b>	Submitted by Student P Student paper	3%
<b>5</b>	Submitted by Student P Student paper	1%
<b>6</b>	Submitted by Student P Student paper	1%



# Stochastic Forensics

- Jonathan Grier
- Black Hat USA 2012
- Insider data theft does not create artifacts
- Can reconstruct activity
- Criticism: Only provides evidence and indications of data theft, and not concrete proof.

**"When you copy, you break that pattern. Because when you copy, you don't cherry-pick, you just get in and get out. And that has a uniform pattern, which is going to look unusual."**



# COMMUNICATION & AWARENESS

# MITIGATION



# ORGANIZATIONAL FACTORS

- Availability and Ease
- Access privileges
- Markings
- Egress Ease
- Undefined policies regarding working from home
- Minimal or Non-existent Consequences for Theft
- Time pressure
- Lack of Training



# WHAT WE CAN DO...

- Provide non-threatening and convenient ways for employees to report suspicions
- Monitor computer networks for suspicious activity
- Ensure security personnel have the tools they need
- Education
- Protect Intellectual Property
- Screen New Employees
- Have a Solid Exit Process



# WHAT DO I DO IF I SUSPECT SOMEONE OF BEING AN INSIDER THREAT?

**Legal Department**

**Supervisor**

**Security Officer**

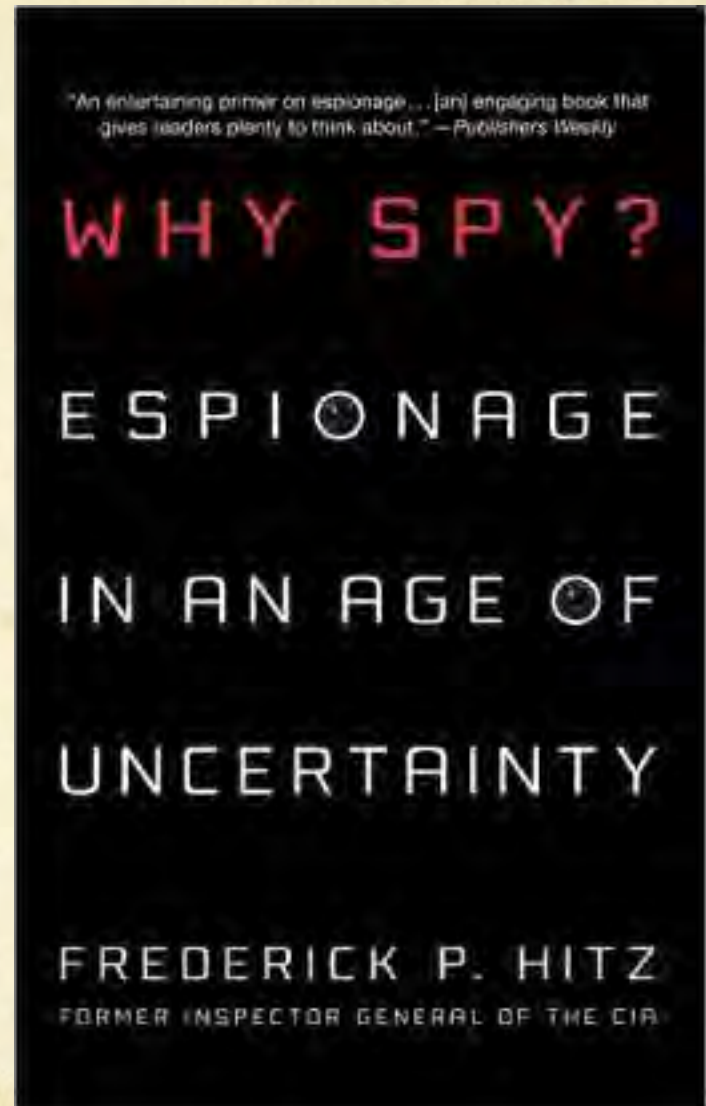
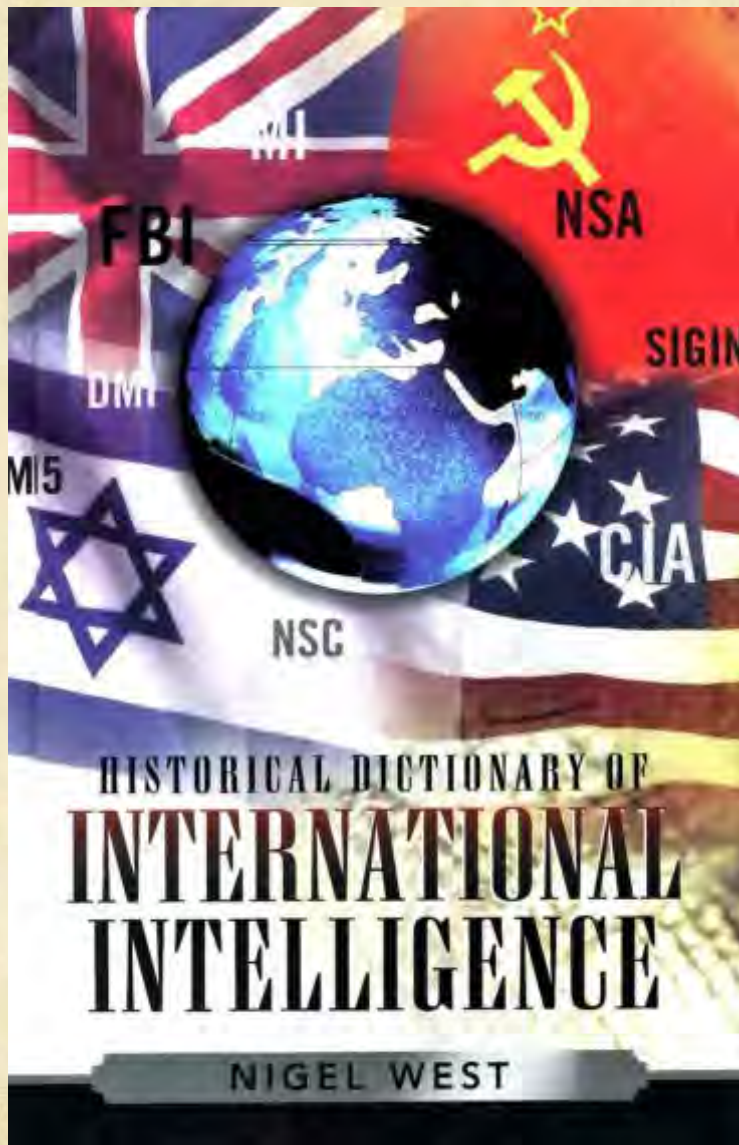
**Trusted Mentor**





# SOURCES





SYNGRESS®

**4 FREE BOOKLETS**  
YOUR SOLUTIONS MEMBERSHIP



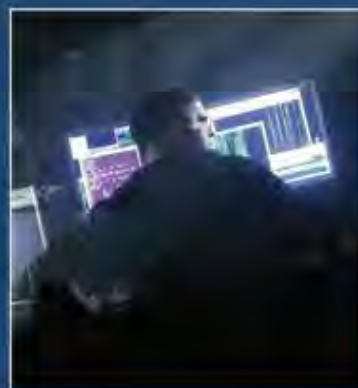
# Enemy AT THE Water Cooler

Real-Life Stories of Insider Threats and  
Enterprise Security Management Countermeasures

"*Enemy of the Water Cooler* is a must read for CIOs and security  
officers everywhere..." —William P. Crowell,  
former Deputy Director of the National Security Agency

**Brian T. Contos, CISSP**

# The CERT® Guide to Insider Threats



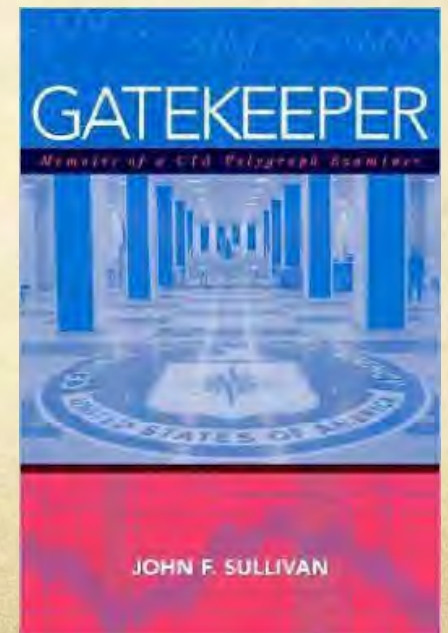
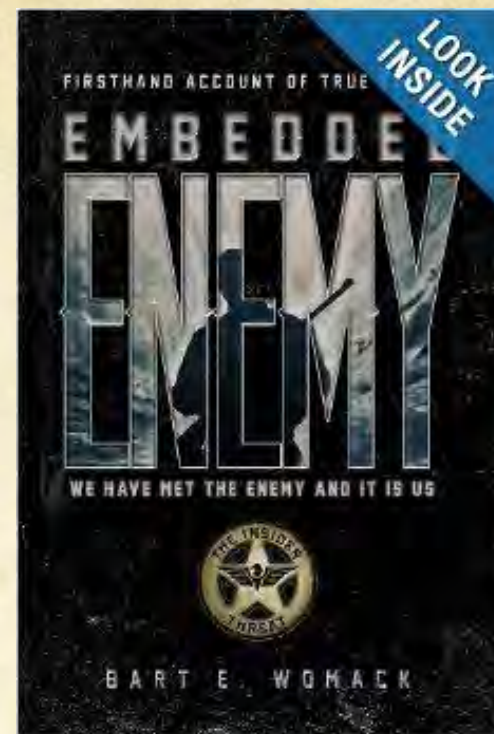
How to Prevent,  
Detect, and Respond to  
Information Technology  
Crimes (Theft, Sabotage,  
Fraud)

SEI SERIES • A CERT® BOOK

**Dawn Cappelli**

**Andrew Moore**

**Randall Trzeciak**



United States of America versus Brian Patrick Regan – Criminal No. 01-045A

United States of America versus Wen Ho Lee – Criminal No. 99-1417

United States of America versus Dongfan “Greg” Chung - Case No.: SACR 08-00024-CJC

Bhattacharjee, Y. (2010, January 25). Tale of a Would-Be Spy, Buried Treasure, and Uncrackable Code | Magazine | WIRED. *Wired.com*. Retrieved from [http://www.wired.com/2010/01/ff\\_hideandseek/](http://www.wired.com/2010/01/ff_hideandseek/)

Harnden, T. (2007, June 7). The spies who loved. . . and lost their jobs. *The Telegraph*. Retrieved from <http://www.telegraph.co.uk/news/features/3632872/The-spies-who-loved.-.-and-lost-their-jobs.html>

OSTROW, R., & CIMONS, M. (1985, July 12). CIA Employee, Ghanaian Held on Spy Charges. *Los Angeles Times*. Retrieved from [http://articles.latimes.com/1985-07-12/news/mn-8825\\_1\\_cia-employee](http://articles.latimes.com/1985-07-12/news/mn-8825_1_cia-employee)

Silverman, B. (2010, February 8). Dongfan "Greg" Chung, Chinese Spy, Gets More Than 15 Years In Prison. *The Huffington Post*. Retrieved July 14, 2014, from [http://www.huffingtonpost.com/2010/02/08/dongfan-greg-chung-chines\\_n\\_454107.html](http://www.huffingtonpost.com/2010/02/08/dongfan-greg-chung-chines_n_454107.html)

**Spotlight On: Insider Theft of Intellectual Property Inside the United States Involving Foreign Governments or Organizations**

By: Matthew L. Collins; Derrick Spooner, Dawn M. Cappelli; Andrew P. Moore, & Randall F. Trzeciak

May 2013 / TECHNICAL NOTE / CMU / SEI-2013-TN-009

**Behavioral Risk Indicators of Malicious Insider Theft of Intellectual Property: Misreading the Writing on the Wall**

By: Eric D. Shaw, Ph.D. & Harley V. Stock, Ph.D., ABPP, Diplomate, American Board of Forensic Psychology

2011 / Symantec White Paper

**Identifying Personality Disorders that are Security Risks: Field Test Results**

By: Olga G. Shechter & Eric L. Lang

September 2011 / Defense Personnel Security Research Center

**Insider Threat Control: Using Plagiarism Detection Algorithms to Prevent Data Exfiltration in Near Real Time**

By: Todd Lewellen, George J. Silowash, & Daniel Costa

October 2013 / TECHNICAL NOTE / CMU / SEI-2013-TN-008

**Catching Insider Data Theft with Stochastic Forensics**

By: Jonathan Grier

2012 Black Hat USA Presentation

**Detecting and Preventing Data Exfiltration Through Encrypted Web Sessions via Traffic Inspection**

By: George J. Silowash, Todd Lewellen, Joshua W. Burns, & Daniel L. Costa

March 2013 / TECHNICAL NOTE / CMU / SEI-2013-TN-012

**Justification of a Pattern for Detecting Intellectual Property Theft by Departing Insiders**

By: Andrew P. Moore , David McIntire, David Mundie, & David Zubrow

March 2013 / TECHNICAL NOTE / CMU / SEI-2013-TN-013

**Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector**

By: Marisa Reddy Randazzo, Dawn Cappelli, Michelle Keeney, Andrew Moore & Eileen Kowalski

2004 / CERT® Coordination Center / National Threat Assessment Center / Software Engineering Institute / United States Secret Service

**Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors**

By: Michelle Keeney, Dawn Cappelli, Eileen Kowalski, Andrew Moore, Timothy Shimeall, & Stephanie Rogers

2005 / National Threat Assessment Center / United States Secret Service / Software Engineering Institute

[www.sei.cmu.edu](http://www.sei.cmu.edu)

For four decades, the Software Engineering Institute (SEI) has been helping government and industry organizations to acquire, develop, operate, and sustain software systems that are innovative, affordable, enduring, and trustworthy.

### National Threat Assessment Center

[www.secretservice.gov/ntac\\_its.shtml](http://www.secretservice.gov/ntac_its.shtml)



The mission of NTAC is to provide guidance on threat assessment, both within the Secret Service and to its law enforcement and public safety partners in the following areas:

- Research on threat assessment and various types of targeted violence.
- Training on threat assessment and targeted violence to law enforcement officials and others with protective and public safety responsibilities.
- Information-sharing among agencies with protective and/or public safety responsibilities.
- Programs to promote the standardization of federal, state, and local threat assessment and investigations involving threats.