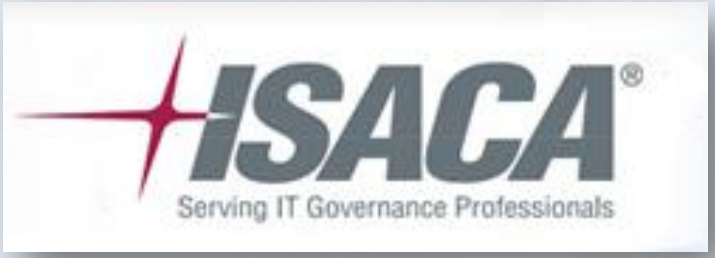
Mitigating the Insider Threat

Paul Williams, MCSE, IAM, IEM
Chief Technology Officer
Gray Hat Research Corporation



ISACA Houston Chapter - Security Seminary

February 21, 2008

Presentation Overview

- How Bad Is The Problem?
- Case History Examples Illustrate Insider Network Vulnerabilities and Effective Insider Defenses
- Insider Threat Mitigation: Assessment, Deterrence, Protection, Alerting, Detection, and Enforcement
- The Insider's Tool of Choice: Network Spy Devices - Weapons of Attack for Hardened Internal Targets
- New Methods of Insider Threat Detection
- Questions & Answers

SPECIAL NOTE:

THE ONLINE HANDOUT VERSION OF THIS SLIDE SHOW CONTAINS A TRUNCATED OUTLINE ONLY OF THIS SESSION.

GRAY HAT RESEARCH CUSTOMER CASE HISTORY EXAMPLES AND PROPIETARY METHODOLOGY SLIDES HAVE NOT BEEN INCLUDED.

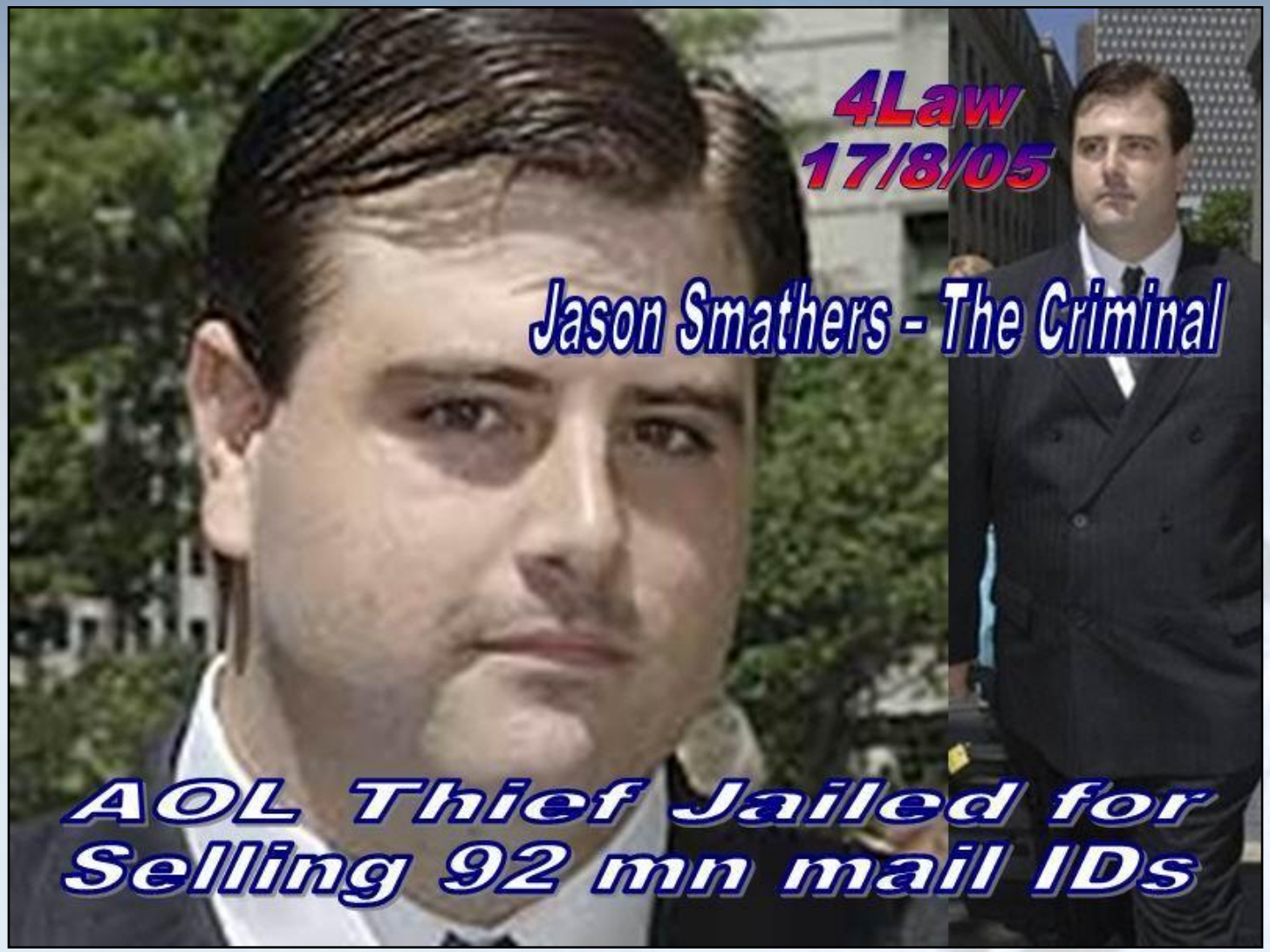
How Bad Is The Problem?

Insider Threats in the News

- The Enemy Within- Geeks, squatters and saboteurs threaten corporate security
- Banks to blacklist rogue workers in fraud fight
- Massive insider bank security breach uncovered in N.J. - 500,000 victims alleged
- 'Stealing from the Collection Plate' -Fraud Magazine
- The Enemy Inside: Insider Theft Costs $400 Billion a Year –CSO online
- Nightmare On Wall Street: USB PaineWebber Suffers Vicious Insider Attack
- Stealing PINs lands former Verizon Wireless employee a prison term
- Company Spy- The Case of the $100 Million Blueprints
- Larry McPhillips hacks company he founded, commits $500,000 fraud
- Former Employee Charged With Intercepting E-Mail, faces up to 15 years in prison
- Employee Trio charged with stealing Coca-Cola trade secrets
- Former Employee Stole $270,000 from Chalmette Bank, was hired by Capital One -FBI

Recent Insider Bank Robbery – Nov. 2007

AOL Network Administrator Sells 92M Records



Bank Vice-President Steals $525,000

Department of Justice

The United States Attorney's Office

Southern District of Texas

News Release

Jan. 10, 2008

FORMER BANK V.P. SENTENCED TO PRISON

(CORPUS CHRISTI, Texas) – Sheri Lynn Yarbrough, 41, a former Vice-President of Commercial State Bank, was sentenced to more than five years imprisonment following her convictions for embezzlement by a bank officer and money laundering, United States Attorney Don DeGabrielle announced today.

At a hearing before Chief United States District Judge Hayden Head, Sheri Lynn Yarbrough was sentenced to 63 months in federal prison for each count, to be served concurrently. Following her release from prison she will remain under court supervision for five years. Yarbrough was also ordered to pay restitution in the amount of $525,710.98.

Yarbrough previously pleaded guilty to one count of embezzlement by a bank officer and one count of money laundering. During her guilty plea, the defendant admitted that while she was employed by Commercial State Bank in Sinton, Texas, she stole more than $525,000 from customer certificates of deposit. She further admitted she moved much of the stolen money through multiple bank accounts in an effort to disguise the source of the funds. Commercial State Bank previously provided full restitution to all depositors whose accounts were affected.

The case was investigated by agents from the Internal Revenue Service, the FBI and the Federal Deposit Insurance Corporation. The case was prosecuted by Assistant United States Attorney Robert D. Thorpe Jr.

Insider Threat Statistics

Hit Ratio Statistics by size of *Company* *

TYPE OF CHECK & RESULT	NUMBER OF EMPLOYEES		
	1-49 Employees	50-999 Employees	1,000+ Employees
Criminal Hit Record	4%	5%	5%
False Information on Resume	48%	50%	53%
Personal Reference (Negative remarks)	7%	10%	7%
Driving Record (1-3 violations)	34%	31%	29%
Driving Record (4 or more violations)	6%	6%	4%
Credit Record with Negative History	34%	47%	42%
Workers Compensation	12%	11%	7%

* Based on American DataBank's research statistics 2002 - 2003.

The Problem Is Widespread

Battlefield Statistics!

- The percentage of resumes and job applications that contain lies and exaggerations has been estimated between 30 and 80 percent. (Security Management Magazine)
- 5% of professional hires have criminal records. (Source: HR Logic)
- 75% of internal theft is undetected. ("How to Identify Dishonesty Within Your Business")
- Several studies estimate employee theft and dishonesty costs U.S. businesses between $60 billion and $120 billion per year, not including the billions spent on protecting against theft. ("How to Identify Dishonesty Within Your Business")
- Insider theft is growing at 15% annually. (Justice Department)
- Employee theft amounts to 4% of food sales at a cost in excess of $8.5 billion annually. 75% of inventory shortages are attributed to employee theft. (National Restaurant Association)
- The Labor Law Industry has increased by 2200%. (Equal Employment Opportunity Commission)
- Employee theft costs between 1/2%-3% of a company's gross sales. Even if the figure is 1%, it still means employees steal over a billion dollars a week from their employers. ("How to Identify Dishonesty Within Your Business")
- One-third of all employees steal from their employers. (Department of Commerce study)
- 30% of business failures are due to poor hiring practices. Annual losses generated by poor hires, absenteeism, drug abuse, and theft amount to $75 billion per year. (U.S. Department of Commerce-Atlanta Business Chronicle.)

Battlefield Stats from: http://www.corporatecombat.com/statistics.html

Insider Threat Mitigation:

Assessment, Training, Deterrence, Detection, and Enforcement

How To Mitigate the Insider Threat

- Implement background checks and drug testing for all employees on a pre-employment basis. Implement random checks for all existing employees (or better)
- Retain a signed Acceptable Network Use Policy agreement for each employee
- Company security policies must be comprehensive and contain specific procedural details. This prevents ambiguity and “wiggle room”
- All employees should be periodically re-trained in the company’s security policies
- Adhere to the Principal of “Least Privilege”: ordinary company users should not have administrative access to their workstations (a network redesign may be necessary)
- Enforce strict Separation of Duties: **all** network Administrator roles and duties can be separated, without exception.
- Implement internal network compartmentalization to contain threats within specific zones, and implement enterprise auditing at each zone’s boundary.
- Deploy enterprise class auditing to provide real time alerting services
- Treat all violators with consistent, predictable enforcement behavior
- Reward employees for identifying internal poor behavior.

Finally, new and improved Personnel test and evaluation methods exist which will be discussed at the conclusion of this section.

New Methods of Insider Threat Detection

Insider Threats Impact All Organizations

Does A Way Exist to Accurately Detect Insider Threats Before They Can Strike, NOT After?

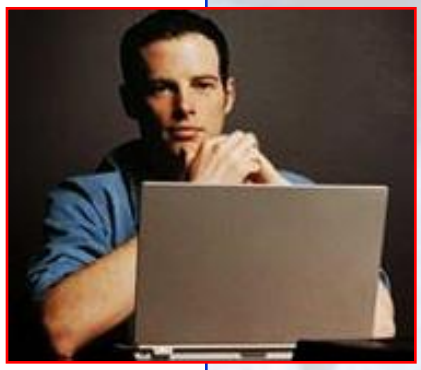
Answer: Fortunately for all of us: **Yes.**

Mitigating the Insider Threat

Our analysis reveals the following mix of positive and negative traits, listed here separately.

On the positive side, Kevin Wily is:

- Driven, [can be a good or bad trait]
- Smart,
- Resourceful, [can be a good or bad trait]
- Dominating, [can be a good or bad trait]
- Relentless, [can be a good or bad trait]
- Talented.



On the negative side, Kevin Wily is:

- Unprincipled,
- Determined,
- Contemptuous of boundaries,
- Disrespectful of authority that does not side with him,
- Manipulative,
- Cunning,
- Deceitful to the extent needed to accomplish his objectives,
- Ruthless to an extent,
- Brilliant in his own areas of specialty, but dangerously unbalanced in his thinking toward his own personal goals and objectives.

Lee Marshall

4.3 Lee Marshall - Risk Assessment Results

4.3.1 Positive Personality Traits

Lee Marshall:

- Cares about matters of technical interest to him and can be driven to succeed if it suits him
- Is capable of high work output, although sometimes because of shortcuts he takes in procedure and process that may be obvious without careful observation/management
- Is capable of perfection in accomplishing tasks of interest to him
- Does not resist change if it aligns with his general interests
- Will experiment with new technologies as it suits him
- Is generally adverse to risk, although with important exceptions.

4.3 Lee Marshall - Risk Assessment Results

4.3.2 Negative Personality Traits

This profile was constructed blind from a remote analysis of the subject's photograph and resume. This analysis later proved to be spot on accurate.

Lee Marshall:

- Has a sloppy side, born out of his concentration on skills and tasks deemed more important to him and combined with disregard or even contempt for tasks and skills deemed "unimportant" or unnecessary
- Will not make an effort to improve on skills he deems unimportant, unless he clearly views an upside in it (most likely), or he sees the opportunity to avoid significant and immediate reproach (less likely)
- Often feels constrained into a course of action or circumstances he wishes he could avoid, and tries to pretend he knows nothing about the subject in question
- May have difficulty verbally relating his true feelings to a supervisor unless considerable effort is made to make him feel comfortable
- Resists change in areas that not of importance or concern to him
- Takes more risks than necessary in accomplishing his work, although typically with such a degree of success that such shortcuts may be overlooked or even go unnoticed
- May despise arbitrary restrain and "rules for no reason" to the point that he may seek to flaunt rules he deems senseless; although always behind the back of superiors, in keeping with his generally risk-adverse nature
- May perceive himself as unencumbered from threats of discharge from employment.

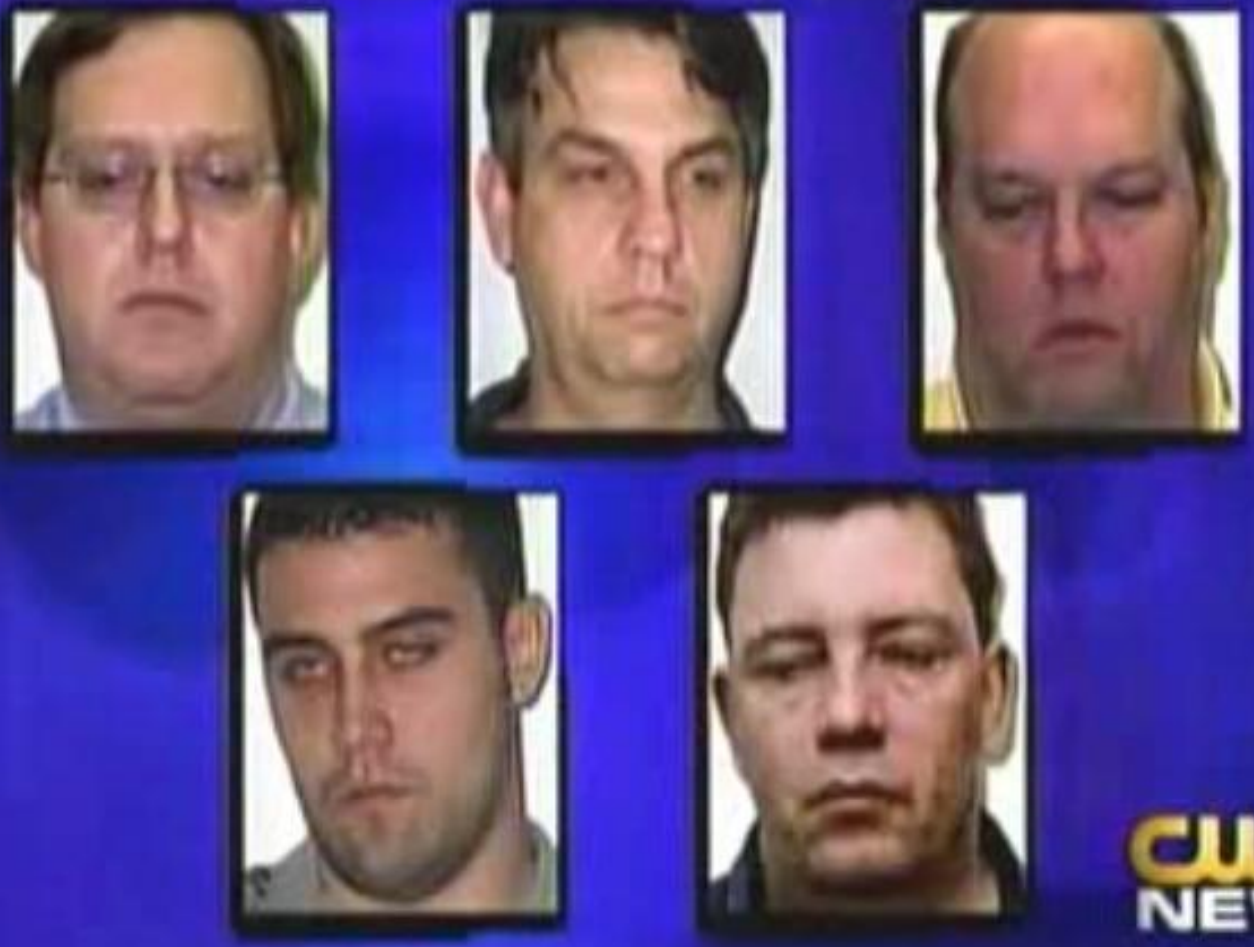
How Does It Work?
Psychological Profiling Introduction

- The Federal Bureau of Investigation's Behavior Science Unit in Virginia conducts the majority of psychological profiling based research of criminals in the United States
- Gray Hat Research has developed its own proprietary system separately from the FBI. Our system is entirely complimentary with the FBI's system.
- It is a proven, effective approach to solving complex cyber crimes, and even predicting criminal behavior well in advance, without relying on prior evidence or even suspicion a crime of any kind
- Profiling may be done through:
  1) In-person or over the phone contact;
  2) Photography analysis;
  3) Resume analysis.
- A combination of all three techniques is highly precise, specific and detailed in the depth and extent of findings
- The process is completely clandestine. Suspects have no way to know that an investigation is even taking place, never mind how or why.

An informative video overview will play next.

Suspects

CW39 NEWS



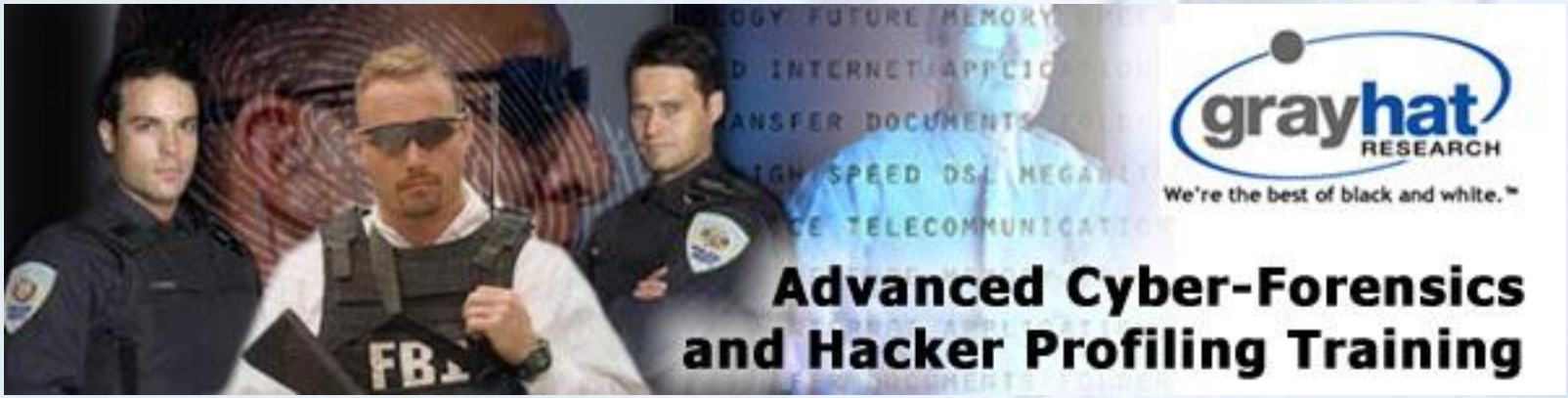
Want To Learn More?

Class Motto for our Advanced Cyber Crimes Investigations Course:

"No logs, no evidence, no suspects, and no obvious place to begin? NO PROBLEM!"

Next Class Date:

- **March 11 - 14: Montgomery College, Houston, Texas**



April 4, 2006 Volume 3, 4th Edition

Finding the Enemy Within:

Psychological Profiling Improves Protection Against Present and Future Insider Threats

by Paul Williams
Gray Hat Research President and Chief Technology Officer

The greatest threat to an organization's information assets is not found in the world of technology. A company's greatest liability is its people: the employees and personnel charged with making the business run.

Whether through negligence, carelessness, circumvention of policy, or deliberate th
assets, interr
risk exposure
physical solu
access can n

you
dentify
before
eed?
ew hire

Leave a Business Card or Sign up for our security newsletter at:

www.grayhatresearch.com

Questions ?

Gray Hat Research Corporation

Join our email list. Sign up at:
www.grayhatresearch.com

Or email: info@grayhatresearch.com

Thank You For Attending!

ISACA Houston Chapter Meeting