A Worst Practices Guide to Preventing Leaks, Attacks, Theft, and Sabotage

Matthew Bunn (with Scott D. Sagan)

27th International Training Course, Sandia National Laboratories
May 17, 2018

Insider Threats: New from Cornell U Press

- Hegghammer & Daehli – Jihadi thinking on nuclear insiders
- Zegart – Ft. Hood shooter (Nidal Hasan)
- Stern & Schouten – Anthrax letters (Bruce Ivins)
- Long – Green-on-blue attacks in Afghanistan
- Bunn & Glynn – Insider security for casinos and pharma
- Bunn & Sagan – Introduction and conclusions – "worst practices guide"
- Part of American Academy of Arts and Sciences "Global Nuclear Future" initiative

http://www.cornellpress.cornell.edu/book/?gcoi=80140100868640

Insider Threats are the Most Dangerous Nuclear Security Problem

- The known HEU and Pu thefts, and most sabotages, involved insiders
  - More real incidents than people often recognize
- Insiders have authorization to go through many layers of the security system
- Insiders are known colleagues
- Insiders may understand key aspects of facility operations and the facility's security system
- Can learn from both nuclear and high-security non-nuclear cases

A Recent Example: Insider Sabotage and a Cleared Terrorist at Doel-4

- August 2014: An insider at Doel-4 reactor in Belgium drains lubricant, destroys reactor turbine
  - ~$200 million damage
  - Investigators unable to find culprit
  - Sabotage not intended to cause radiation release
- Long before, Ilyass Boughalab had access to vital area
  - Passed security clearance review in 2009
  - In late 2012, left to fight for terrorists in Syria (reportedly killed later)
  - Later convicted as part of "Sharia4Belgium" terrorist group

Ilyass Boughalab
Source: Kristof Pieters

Cognitive, Organizational Biases Undermine our Ability to Cope with Insider Threats

- Insiders are the most serious threat to nuclear, intelligence, and many other organizations
- But insiders are trusted, authorized employees
- Cognitive dissonance, affect bias, illusion of control lead people to ignore warning signs
- Organizational dysfunction adds disincentives to reporting, acting on warning indicators
- Even seemingly obvious “red flags” are sometimes ignored

Doel-4 nuclear power plant – sabotaged by an insider in 2014

Lesson #1: Don't Assume that Serious Insider Problems are NIMO (Not In My Organization)

Case Study I: Indira Gandhi Assassination

- Death threats against Gandhi and her family after 1984 crackdown on Sikh uprising
- Extra security personnel deployed to Gandhi's residence
- Gandhi protested suggestion that Sikh bodyguards should be placed only on outside perimeter of compound
- Gandhi assassinated by two Sikh guards on October 31, 1984

Beant Singh and Indira Gandhi

Lesson #1: Don't Assume that Serious Insider Problems are NIMO (Not In My Organization)

Case Study II: Edward Snowden

- Able to download vast numbers of highly sensitive files – because insiders were not being closely monitored
- Clapper: "Our whole system is based on personal trust."
- Booz Allen Hamilton CEO: "Our most trusted colleagues and friends have this in common. We can count on them… Booz Allen Hamilton is trusted in that way."

Edward Snowden

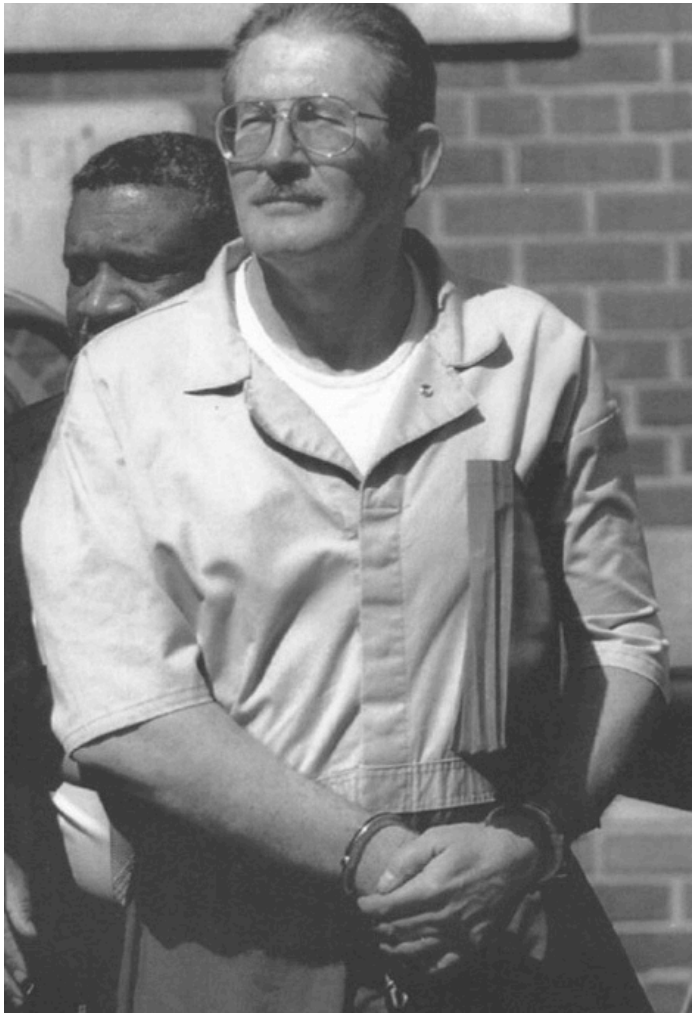
A Special Problem for Lesson #1: Rapid Radicalization

- Beant Singh was a loyal guard for years – until weeks before Gandhi's assassination
- Ilyass Boughalab was radicalized in months – *after* his background check
- German analysis of foreign fighters – many radicalized in <1 year (13% no indicators until showed up in Syria)
- Numan Haider – Australian teenager, radicalized in months

Numan Haider's Facebook page

Lesson #2: Don't Assume That Background Checks Will Solve The Insider Problem

Case Studies: Aldrich Ames, Leonid Smirnov, and Northern Bank Theft



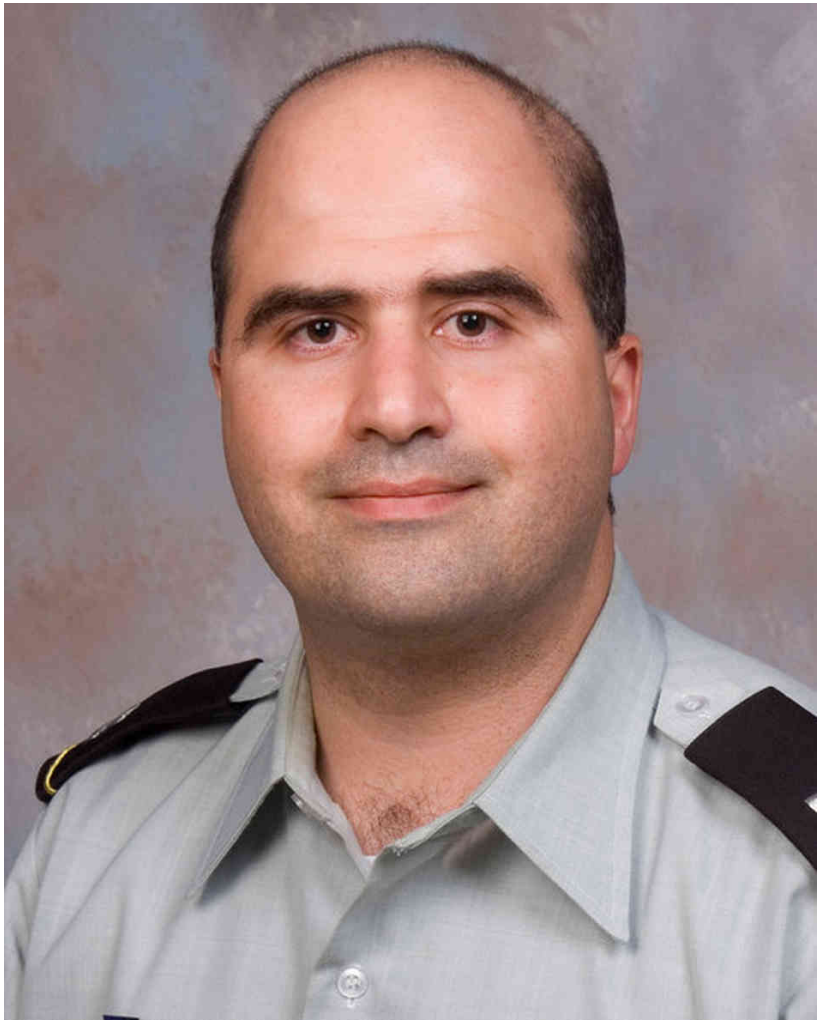
Aldrich Ames

- Background checks are not perfect
  - Aldrich Ames passed lie detector tests
  - Leonid Smirnov (1992 HEU thief) was considered a trusted employee
- Loyal employees can be coerced
  - 2004 Northern Bank theft
- People may be radicalized *after* they pass a check – and quickly

Lesson #3: Don't Assume That Red Flags Will Be Read Properly

Case Study I: 2009 Fort Hood Shooting

- Hasan voiced radical beliefs and emailed Anwar al-Awlaki – a known terrorist
- Reasons for failure to act
  - Army system for reviewing officers' performance failed to forward relevant information
  - Social shirking + the Army's needs
  - Colleagues feared being accused of bias
  - Intelligence officer interpreted al-Awlaki emails as "research"
  - Misunderstanding on who was following up investigative leads

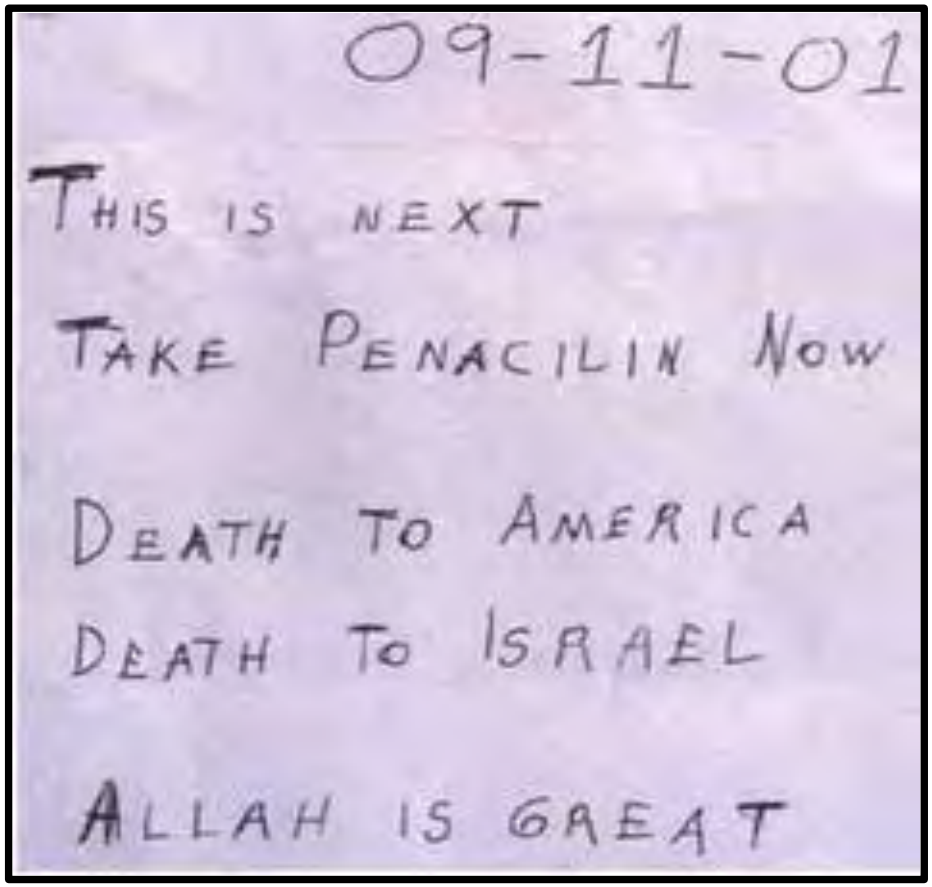


Maj. Nidal Malik Hasan

Lesson #3: Don't Assume That Red Flags Will Be Read Properly

Case Study II: 2001 Anthrax Letters

- Bruce Ivins offered many red flags
  - Therapists found him highly dangerous (records never reviewed)
  - He complained about his own dangerous paranoia (never reported)
  - Subordinates reported his bizarre behavior, and being afraid of him (no action taken)
  - Long-standing eccentricity "immunized" the organization to noticing concerning behavior



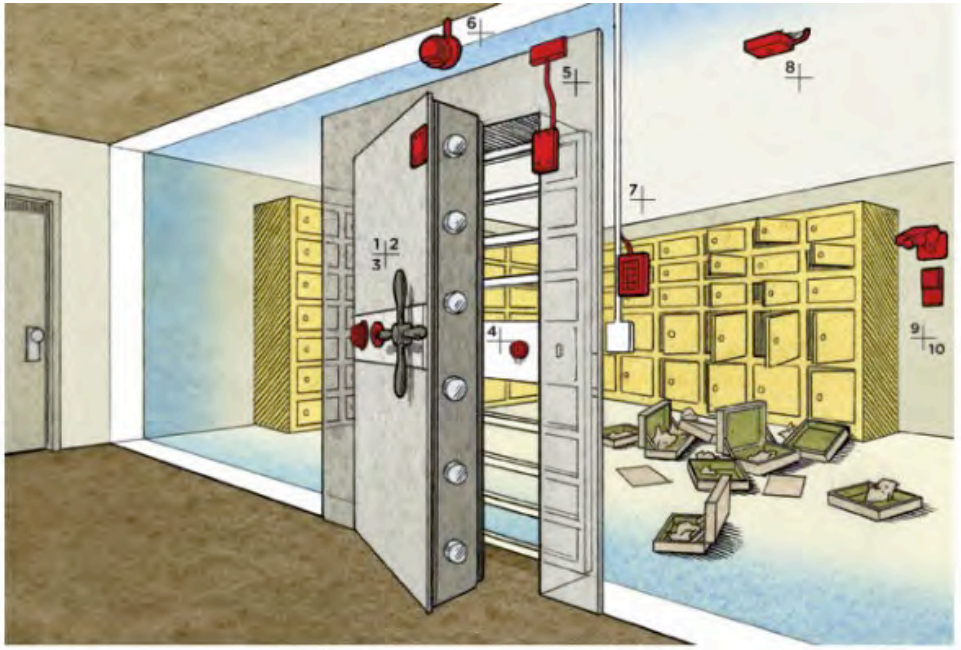
Text of Anthrax Letter

Lesson #4: Don't Assume That Insider Conspiracies Are Impossible

Site of 2004 Northern Bank Theft

- Recent survey of nuclear security experts:
  - Single insider seen as credible, insider conspiracies generally not
- Yet: insider conspiracies not unusual
  - *More* common than single insiders in Sandia study of major heists
- Where practical, security systems should be designed to cope with more than one insider

Lesson #5: Don't Rely on Single Protection Measures



The Door
1. Combination dial (0-99)
2. Keyed lock
3. Seismic sensor (built-in)
4. Locked steel grate
5. Magnetic sensor
6. External security camera

The Vault
7. Keypad for disarming sensors
8. Light sensor
9. Internal security camera
10. Heat/motion sensor (approximate location)

2003 Antwerp Diamond Center Heist
Source: Wired

- Portal monitors can be defeated or gone around
- Seals can be defeated
- Staff often fail to report concerning behavior
- Effective security requires comprehensive, multi-layered approach
- Realistic testing and creative vulnerability assessment are essential

Lesson #6: Don't Assume that Organizational Culture And Disgruntlement Don't Matter

Case Study I: Y-12 Incursion

Graffiti from Y-12 Break-In

- 2012: 82-year-old nun and two other protestors enter Y-12 facility
  - Passed through 3 alarmed fences, setting off multiple alarms – no one responded for extended period
  - New instrusion detection system setting off 10x as many false alarms
  - Cameras to allow guards to see cause of alarm had been broken for months
  - Major breakdown in security culture

Lesson #6: Don't Assume that Organizational Culture And Disgruntlement Don't Matter

Case Study II: Chelsea Manning

Chelsea Manning

- Manning was a classic disgruntlement (and emotional disturbance) case
  - A dawning transgender identity in the "don't ask don't tell" military
  - Had to be restrained after being told she would lose her weekly day off for lateness
  - Began downloading 3 weeks later

Lesson #6: Don't Assume that Organizational Culture And Disgruntlement Don't Matter

Case Study III: Cyber Sabotage

Source: Cyber Crime News

- One study found 92 percent of the cyber sabotage cases in the sample came after a negative work event
- Over half of the perpetrators were already seen by others as disgruntled
- Simple steps – listening, validating, sometimes action on complaints – can greatly reduce disgruntlement

Lesson #7: Don't Forget that Insiders May Know About Security Measures and How to Work Around Them

Case Study I: Robert Hanssen

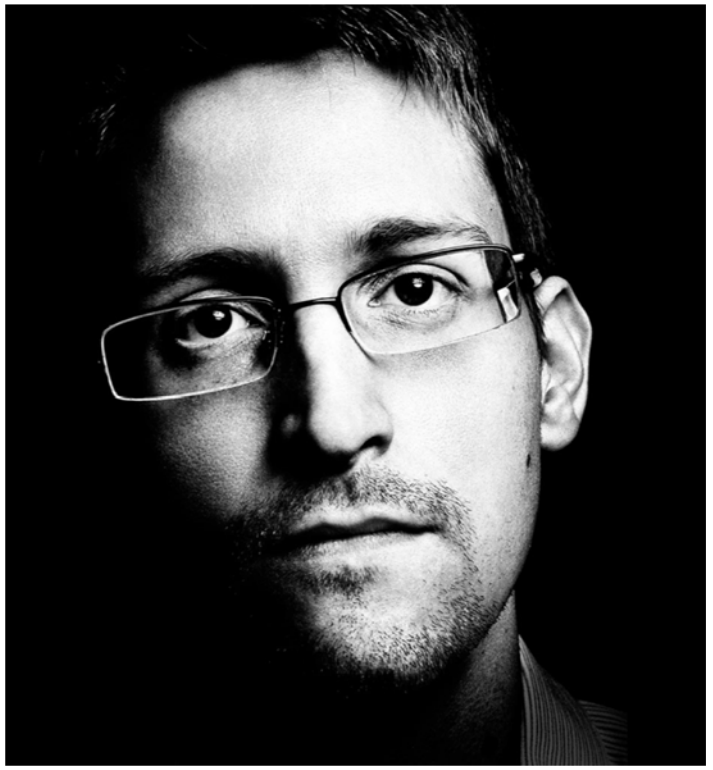
- Senior FBI counterintelligence agent, arrested February 2001
- Convicted on 15 counts of espionage
- Leaked photocopies and disks to Russia for 22 years, compromised many agents
- Able to monitor internal FBI investigations, alter espionage practices to avoid detection, and avoid polygraph tests

Robert Hanssen

Lesson #7: Don't Forget that Insiders May Know About Security Measures and How to Work Around Them

Case Study II: Edward Snowden

- Snowden was an NSA systems administrator – watching for security weaknesses was one of his tasks
- The Hawaii site he arranged to be transferred to had not yet installed software to monitor unusual activity
- So Snowden was able to use simple "web scraping" tools without detection



Edward Snowden

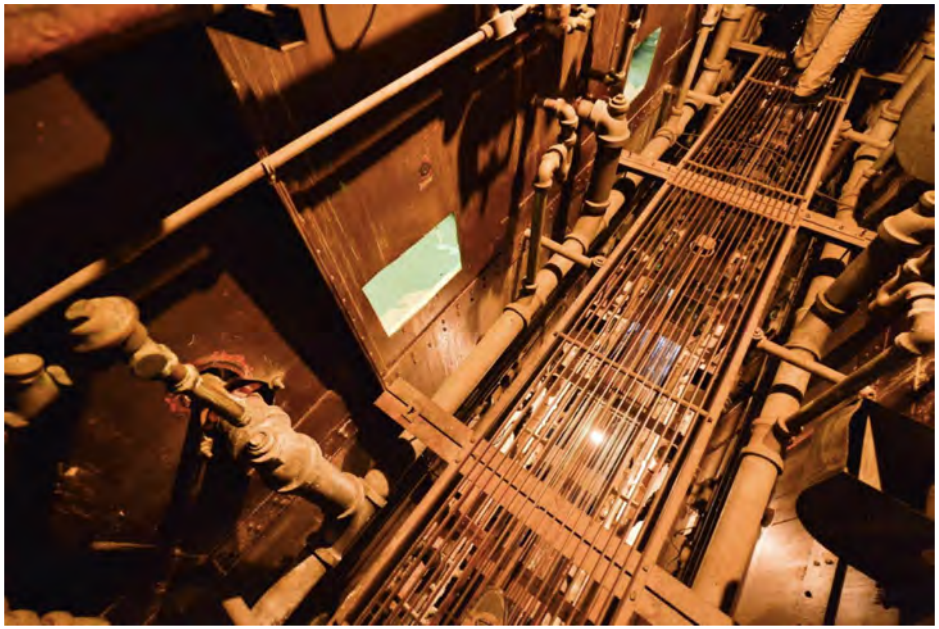
Lesson #8: Don't Assume That Security Rules Are Followed

- In both the United States and Russia, multiple cases of:
  - Guards patrolling without ammunition in their guns
  - Guards turning off intrusion detectors
  - Staff violating security rules for convenience
- Real practice often looks much different than the practice prescribed in the rule book

Propped-open security door in Russia.
Source: GAO, 2001

Lesson #9: Don't Assume That Only Consciously Malicious Insider Actions Matter

Case Study: 2015 New York Prison Break



Hole next to catwalk, Clinton Correctional Facility

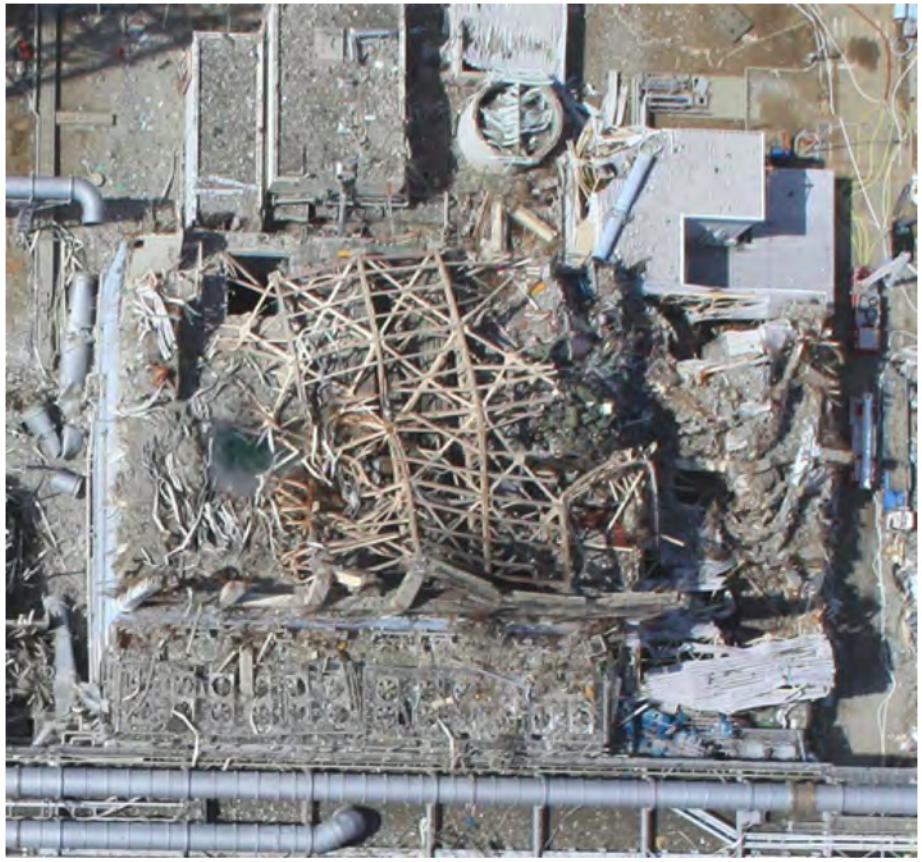
- Guard Gene Palmer developed relationship to get information from inmates
- Provided tools he saw as innocent
- Provided hamburger in which another insider had hidden tools

Lesson #9: Don't Assume That Only Consciously Malicious Insider Actions Matter

A key issue: Cyber

- Inadvertent insiders common in cyber cases
- Individuals click on a link, download a file, bring in a USB drive… and attackers get in
- "Phishing" attacks are becoming more and more sophisticated, individualized
- Separating networks from the internet is important – but not enough
- *Intentional* cyber insiders are also a key issue

Lesson #10: Don't Rely Only on Prevention and Assume Mitigation Doesn't Matter



Source: Air Photo Service, Japan

Examples:

- Sabotage: safety measures and emergency response can reduce effect
- Theft: Material in big and heavy forms, with low concentrations of nuclear material, immediate detection and pursuit, can reduce chance material could be used in a bomb

Nuclear Caveat: Few Jihadist Writings or Actions on the Nuclear Insider Possibility

Source: *Time*

- Hegghammer and Daehli provide new data on jihadi writings, actions
- Mentions of nuclear tactics are rare
- Mentions of nuclear insider possibilities are nonexistent
- No known cases of jihadis actively recruiting nuclear insiders for theft or sabotage

Caveat to the Caveat: Disturbing Hints of the Potential for Nuclear Insiders

Source: ISIS

- Nearly all known nuclear thefts or sabotage incidents appear to have been perpetrated by or with help from insiders
- Jihadists routinely use insiders (including coerced insiders) in other contexts
- Case of Ilyass Boughalab (cleared insider at Belgian nuclear plant, left to fight for terrorists) highlights potential

Insider threats: What should organizations do?

- Build high-performance and high-vigilance culture – everyone understands that security is their job too
- Build a comprehensive, multi-layered approach to reducing insider threats
  - Maximize the scale and complexity of challenges insider adversaries would have to overcome
- Include regular assessment, testing, “red teaming” as a key part of the insider program
- Design approach within the context of the laws, culture of your country and organization
  - Need to balance maintaining vigilance with fostering atmosphere of trust, cooperation needed for high performance

Insider threats: What should organizations do? (II)

- A comprehensive approach should include:
  - Thorough background checks before access
  - Ongoing monitoring of behavior
  - Requirements, incentives to report concerning behavior, potential vulnerabilities
  - Effective training – with real stories
  - Minimizing human access to vital areas, materials, information
  - Continuously monitoring, controlling, and accounting for vital areas, materials, information
  - Effective investigations, responses to reports – seen as fair and reasonable by staff

A Worst Practices Guide to Preventing Leaks, Attacks, Theft, and Sabotage

http://www.belfercenter.org/publication/insider-threats

Lesson #8: Don't Assume That Security Rules Are Followed

Case Study: Wackenhut Corporation Exercises

Y-12 National Security Complex

- January 2004: DOE Inspector General finds that Wackenhut Corporation had been cheating on security exercises at Y-12
- Management told security guards about the plans for mock attacks
- Guards planned defense and strategically placed obstacles
- Best guards put on duty and number of protective personnel on shifts augmented
- Guards tampered with exercise monitoring equipment