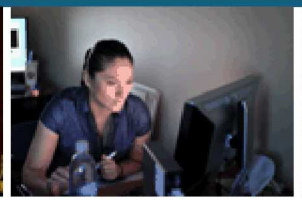
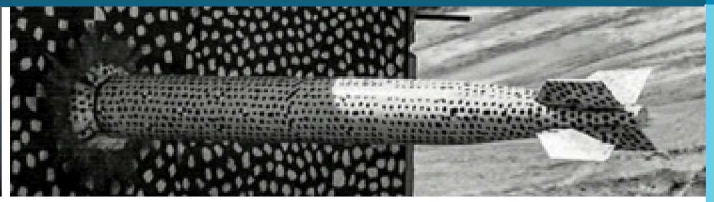
SAND2020-6560C

A New Approach to Insider Threat Mitigation: Lessons Learned from Counterintelligence Theory





Noelle J. Camp and Adam D. Williams

Sandia National Laboratories

Sandia National Laboratories is a multimission laboratory managed and operated by National Technology & Engineering Solutions of Sandia, LLC, a wholly owned subsidiary of Honeywell International Inc., for the U.S. Department of Energy's National Nuclear Security Administration under contract DE-NA0003525.

Insider Threat Literature Review

- According to the IAEA, an insider is defined as: **"an adversary with authorized access to a nuclear facility, a transport operation, or sensitive information."**

- IAEA Nuclear Security Series No. 8 informs current practices for insider threat mitigation (ITM)
  - Provides "general guidance…on prevention of and protection against insider threats"

- Fewer than 10 real-world case studies of insider events within nuclear facilities in the public domain
  - Limits ability to effectively leverage lessons learned from historical insider cases

- Nuclear security professionals have sought insights from other comparable industries:
  - Casino and pharmaceutical industries
  - High-value jewelry heists

2019 INMM Paper, "Preliminary Results from a Comparative Analysis of Counterintelligence and Insider Threat in Nuclear Facilities"

- **Premise:** Counterintelligence (CI) similar to ITM in terms of:
  - High security atmosphere
  - High-value targets
  - Focus on human vulnerabilities
  - Use of preventive & protective mitigation measures
- **Method:** Analysis of ten CI case studies based on a seven criteria rubric for insights applicable to ITM in the nuclear industry
- **Findings:** Notable trends across the ten case studies with potential implications for ITM

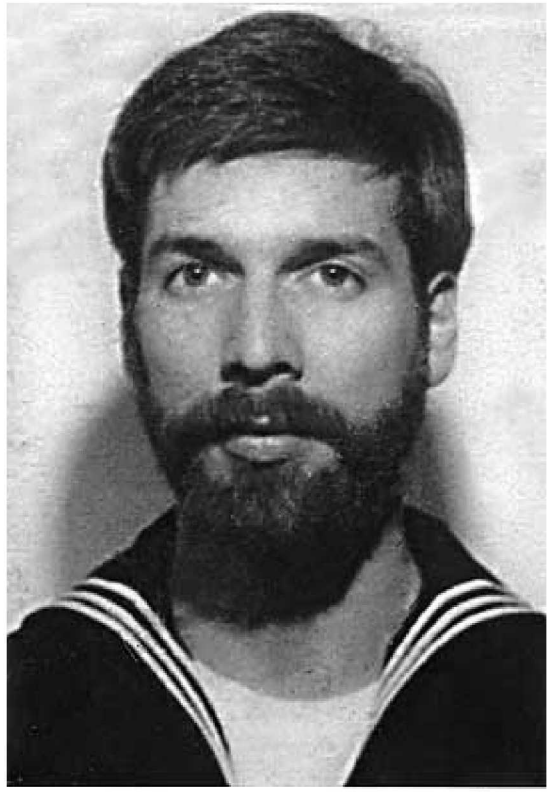
Rubric Criteria	Notable Trends
Position/title of individual	Types of position and level of authority varied widely
Motivation(s)	7/10 cases were motivated by the prospect for financial gain
Recruitment/transition into intelligence collection	Majority of cases volunteered to spy
Mechanisms for accessing sensitive information	Most spies accessed information over the course of their normal duties
Maturity of the "reporting culture"	Underdeveloped in most cases; Strong reporting culture contributed to investigative success
Impact of "preventive" & "protective" measures	Failure patterns in background investigations and security were common
Impact of investigative measures	Electronic and/or physical surveillance measures were among the most popular investigative measures

Building on the Initial Analysis

- **Key Question:** Are trends in the 10 CI case studies empirically present in nuclear insider threat cases?
  - ***If yes*** → Further demonstrate that CI is a useful corollary to ITM
  - ***If no*** → Understanding the differences may help identify what lessons can be leveraged & where ITM is unique
- **Method:** Compared two case study data sets against evaluation rubric
  - Dataset 1: ***10 CI case studies*** from the 2019 INMM paper
  - Dataset 2: ***7 insider threat case studies*** derived from King's College London and LANL study

Dataset 1		Dataset 2	
SNL1	Ana Montes	KCL1	Leonid Smirnov (Luch Scientific Production Association)
SNL2	Glenn Michael Souther	KCL2	David Learned Dale (GE Nuclear Power Plant)
SNL3	Sharon Scranage	KCL3	Multiple cooperative insiders (Elektrokhimpribor)
SNL4	Clyde Lee Conrad	KCL4	Rodney Wilkinson (Koeberg)
SNL5	Jim Nicholson	KCL5	A. Kalinovsky (Radioisotope Factory No. 45)
SNL6	Aldrich Ames	KCL6	Unknown insider (Doel 4 Nuclear Power Plant)
SNL7	Elyesa Bazna	KCL7	Alex Maestas (Los Alamos)
SNL8	Fritz Kolbe	–	–
SNL9	Boris Morros	--	--
SNL10	Stig Wennerstrom	--	--

Case Study In-Depth: Glenn Michael Souther



- **Position/Title:** Navy photographer, later Reservist at secure facility
  - Insiders may use promotions or lateral moves to increase opportunity for malicious action
- **Motivations:** Disgruntlement, ideology, money
- **Recruitment:** Volunteered to Soviet intelligence services
- **Mechanism for Accessing Information:** Normal duties; Took advantage of lax security to obtain additional information
  - Monitoring and a two-person rule to prevent a single individual from accessing highly classified material alone could have benefited the facility
- **Reporting Culture:** Souther's colleagues failed to report multiple indicators of espionage such as unusual work hours, undue affluence, criminal behavior, and suspicious foreign travel
- **Preventive/Protective Measures:** Failure of background investigation
- **Investigative Measures:** Investigators discounted reports from Souther's ex-wife; botched initial interview leading to Souther's defection

Results – Dataset 1

Case No.	Position of individual	Motivation(s)	Recruitment into intelligence	Mechanisms for accessing information	Maturity of the "reporting culture"	Impact of "preventive" & "protective" measures	Impact of investigative measures
1	Counter-intelligence Officer, CIA	Financial	Volunteered to Soviet contacts	Gained access based on his counterintelligence responsibilities	A CIA colleague reported Ames' undue affluence in 1989	Preventive (failure of hiring practices; failed background investigation)	Successful arrest and prosecution (with surveillance)
2	Valet for British Ambassador to Turkey	Financial	Volunteered through German embassy	Stole documents from safe in Ambassador's home	Despite awareness of unusual behavior, was never reported by colleagues	Preventive (failed background investigation) Protective (failure to secure classified information)	Investigation suffered from inter-service rivalries
3	U.S. Army Sergeant First Class	Financial, Ego	Recruited by Hungarian-born supervisor	Stole documents available to him as the custodian for classified documents	Despite several red flags (wealth, attempted recruitment of others), no reporting	Preventive (failure of reinvestigations) Protective (failure to secure classified information; failure to address networks)	Despite inter-agency challenges, successful arrest of individual and other members of the spy ring
4	Diplomat, German Foreign Ministry	Ideology	Volunteered as a "walk-in" to the embassy	Copied information from classified cables accessed during normal duties	Colleagues overlooked indicators, including anti-German views and suspicious contacts	Preventive (failure to address indicators) Protective (failure to secure classified information)	German intelligence unaware of loss and failed to launch an investigation
5	Senior Analyst, Defense Intelligence Agency	Ideology	Recruited by Cuban intelligence	Memorized classified information accessed during normal duties; sought to expand access to information	After receiving an educational CI brief, a colleague reported suspicions to a CI professional	Preventive (failure of background investigation) Protective (failure of compartmenting; success of education)	Successful interagency cooperation (with physical and electronic surveillance) resulted in arrest
6	Hollywood film/music producer	Blackmail, financial	Recruited by Soviets with financial aid to family	Spotted/assessed other contacts in Hollywood for recruitment	There is no indication activities were reported to U.S. authorities	N/A: A unique case with no access to classified information	Served as a FBI double agent
7	CIA Officer, instructor at "The Farm"	Financial, Ego, Disgruntlement	Volunteered to Soviet contacts	Accessed names and bio data as instructor at "The Farm"	Failure to report undue affluence and suspicious behavior	Protective (success of polygraph; successful reports; failure to address networks)	Successful investigation
8	Operations Support, CIA in Accra, Ghana	Love/ Seduction, Blackmail	Recruited by her Ghanaian lover	Information obtained from CIA files at the embassy and cable traffic	No timely report of inappropriate relationship with foreign national	Preventive (failure of training; success of reinvestigation) Protective (failure of reporting)	Success via routine polygraph, lured handler to U.S. for arrest
9	U.S. Navy Reservist	Financial, ego, ideological, disgruntlement	Volunteered while stationed abroad in Italy	Removed classified information from U.S. Navy reserve facility where he worked	Coworkers failed to report indicators (e.g., undue affluence, suspicious travel)	Preventive (failed background investigation) Protective (failure to secure classified information)	Failed investigation, individual escaped to the Soviet Union
10	Swedish Air Force Col. & diplomat	Financial, ego, disgruntlement	Volunteered to Nazi Germany/ Soviet Union	Photographed classified documents accessed as an attaché	No report by colleagues, reported by maid	Preventive (failure of biases)	Successful investigation & arrest (with surveillance)

Results – Dataset 2

Case no.	Position of individual	Motivation(s)	Decision for Action(s)	Mechanisms for accessing material	Maturity of the "reporting culture"	Impact of "preventive" & "protective" measures	Impact of investigative measures
1	Chemical engineer	Financial	Reduction in pay due to collapse of USSR; inspired by newspaper account of nuclear theft	Removed small quantities of HEU while colleagues were out of the room	No evidence to suggest that anyone at the facility was aware of his activities	Protective (failure of two-person rule, failure of materials accounting, failure of radiation detection)	Facility unaware that the material was missing; arrested in a chance encounter
2	Chemical technician (temporary)	Financial	Brother claimed he was depressed due to temporary job ending	Showed driver's license to access restricted area; unlocked door allowed access into Uranium Store	Colleagues did not question the insider's presence although he was not scheduled to be at work and accessed restricted areas	Protective (failure of access control, failure of physical protection system)	Successful FBI investigation resulting in arrest
3	Multiple collaborating insiders	Financial	Reduction in pay due to collapse of USSR	Diverted and diluted 5-10% of isotope solution; colluding insiders took advantage of knowledge and access in many areas	Colleagues at the plant failed to report, justifying their actions because "there was no other way … to make money"	Protective (failure of reporting culture, failure of material accounting practices)	Successful investigation based on indicator of undue affluence resulted in arrest
4	Safety Officer (temporary)	Ideological	Encouraged by African National Congress to carry out attack	Smuggled mines into facility using wine decanters; carried into reactor room via ventilation system; set fuse to 24-hour delay	Suspicious onsite behavior including drunkenness went unreported	Preventive (failure of hiring practices) Protective (failure of access control systems, failure to act on threat assessment)	ANC immediately claimed responsibility; perpetrator granted amnesty after end of apartheid regime
5	Director of Radioisotope Factory	Financial	Reduction in pay due to collapse of USSR	Used senior position at facility to order staff to falsify customs forms to disguise Ir-192 as a different isotope	Coerced subordinates into collaboration	Protective (failure of reporting culture, failure of training)	Successful investigation leading to arrest after customs officials noticed discrepancy in radiation levels
6	Unknown	Potential disgruntlement or ideology (speculated)	Possible tie to Islamic extremist organization	Emergency oil drain valve opened and act concealed, but unknown how this occurred	Unknown	Protective (assumed failure of access control, security training, employee incentives, two-person rule)	Failed investigation; perpetrator has never been identified
7	Technician	Financial	Unknown	Accessed contaminated gold during normal duties; attempted to decontaminate before leaving the building with gold in a plastic bag	No evidence that colleagues were aware of his activities	Protective (success of radiation portal monitor)	Successfully arrested and prosecuted after radiation portal monitor detected the material

Comparing the Datasets

Position/Title

- Both datasets included a wide variety of positions, ranging from very high to very low authority
  - Individuals with high levels of authority in both datasets leveraged their authority
  - Low organizational status may have enabled insider activity to go unnoticed

- Both datasets included an example of multiple collaborating spies/insiders at different levels of the organizational hierarchy working together
  - In these cases, varied access, authority, and knowledge was an asset to the group

- In Dataset 2, two cases included a temporary contractor
  - Temporary nature of the work likely shaped the timeline (potential motivation for David Learned Dale's theft)

Comparing the Datasets

Motivations

- Financial motivation was most common in both datasets
  - Cases in both datasets demonstrated undue affluence through lavish purchases
  - In Dataset 2, several insiders committed malicious acts for relatively modest financial ambitions
- Other motivations present in both datasets included ideology and disgruntlement

Recruitment/Decision for Action

- Most cases across both datasets were internally motivated
- Both datasets included examples of major life events as "triggers" for malicious activity
  - Triggers included divorce, denied promotion, reduction of salary and termination of contract
  - Suggests that events in an individual's personal life may affect the decisions he or she makes in the workplace

Comparing the Datasets

Mechanisms for Accessing Material/Information

- Majority of insiders and spies leveraged normal, everyday access
  - Tracking anomalies may be insufficient as malicious acts may be camouflaged by ordinary responsibilities
- In one CI case and one ITM case, individuals physically broke into a restricted area
  - In both cases, the spy/insider did not have another method of obtaining sensitive information or material

Maturity of Reporting Culture

- Reporting culture across both datasets was weak; no successful examples of reporting culture in Dataset 2
- In Dataset 1, successful reporting culture generally resulted in positive outcomes for the investigation
  - Suggests potential benefit from more robust facility-wide training and user-friendly reporting systems

Comparing the Datasets

Impact of Preventive/Protective Measures

- Failures of background investigations occurred in both datasets
  - **Dataset 1**, investigations failed to uncover past drug use, falsified education, anti-U.S. views, and criminal history
  - **Dataset 2**, it is unclear how many of the insiders received an initial/subsequent (re)investigation

- Both datasets also exhibited failures of protective measures
  - **Dataset 1**, typically related to the inadequate storage of information, either lapses in physical storage or practices
  - **Dataset 2**, often manifested as physical failures, including of the physical protection and access control systems

Investigative Measures

- Diversity of approaches and outcomes made it difficult to discern useful patterns during analysis
  - **Dataset 1**, physical and electronic surveillance was commonly used to gather evidence
  - **Dataset 2**, no trends, but portal monitors and customs enforcement were used successfully in one-off cases

Conclusions

- Many of the same trends appeared across both the counterintelligence and insider threat datasets
  - Supports conception of counterintelligence as a useful corollary for insider threat mitigation

- Counterintelligence case studies may be used as an effective teaching tool for insider threat education and in limited cases may even serve as an analytical proxy

- CI practices may provide useful lessons for nuclear security practitioners, particularly in the areas of cultivating reporting culture and improving insider threat investigations