SAND2020-6258C

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

Noelle J. Camp & Adam D. Williams
Sandia National Laboratories*, Albuquerque, NM, USA, [ncamp; adwilli]@sandia.gov

Abstract

According to the International Atomic Energy Agency's (IAEA) Information Circular (INFCIRC) 908, because "insiders possess access, authority and knowledge … [they] pose an elevated threat to nuclear security." Insiders, witting or unwitting, working together or alone, possess the opportunity to cause significant damage to nuclear facilities through sabotage or unauthorized removal of nuclear or radiological material. In response to this global threat, INFCIRC/908 pledged nearly 30 countries to establish and implement a range of national-level measures to better mitigate insider threats at nuclear facilities. However, the lack of publicly available insider case studies involving nuclear facilities makes causal analysis and pattern recognition difficult. Some insider threat researchers and practitioners have leveraged lessons from other disciplines, including the casino and pharmaceutical industries, to address this challenge.

One untapped discipline with conceptual and practical similarities for eliciting insider threat mitigation insights is counterintelligence, defined by United States Executive Order 12333 as "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations." Both counterintelligence and insider threat mitigation seek to protect high-value assets from malicious, intentional human actions. Each discipline must identify perpetrators from individuals with access rights that give them a privileged position compared to a traditional 'outsider' threat. Additionally, the consequences of failed counterintelligence and insider threat mitigation activities can both result in grave damage to national security.

This paper builds on initial analysis conducted in the 2019 INMM conference paper, *Preliminary Results from a Comparative Analysis of Counterintelligence and Insider Threat Mitigation in Nuclear Facilities*, which evaluated ten counterintelligence case studies for application to insider threat based on a seven criteria rubric. This paper furthers the analysis by evaluating seven insider threat case studies within nuclear and radiological facilities to provide insight into whether trends identified in the counterintelligence case studies are empirically present within the limited set of historical insider case studies in the nuclear field. The paper outlines a comparison rubric and analytical framework, identifies trends and insights across the motivations, characteristics, actions, and investigations applicable to insider threat mitigation, and provides lessons for potentially improving insider threat programs at nuclear facilities.

Introduction

Current global practices for insider threat mitigation in nuclear and radiological facilities are based on International Atomic Energy Agency (IAEA) best practices, most notably Nuclear Security Series No. 8[1], that provides "general guidance to the competent authority and operators on prevention of and protection against insider threats." However, there are few real-world case studies of insider events within nuclear facilities in the public domain, limiting the ability of nuclear security professionals to effectively leverage lessons learned from historical insider cases. The most thorough account of nuclear and radiological insider threat cases, totaling seven case studies, was developed by King's College of

[1] International Atomic Energy Agency, *Preventive and Protective Measures against Insider Threat: Implementing Guide*, Security Series No. 8 (Vienna: IAEA, 2008), 2.

London (KCL) and Los Alamos National Laboratory in 2015.[2] The lack of publicly available case studies has led the nuclear security community to seek insights from other industries, including a 2013 Managing the Atom (Harvard University) study on insider threat mitigation best practices within the casino and pharmaceutical industries[3], a 2015 Sandia National Laboratories (SNL) study examining lessons from 23 attempted and successful heists within high-security, high-value industries,[4] and a 2014 American Academy of Arts & Sciences sponsored investigation of diverse case studies that culminated into a "Worst Practices Guide to Insider Threat."[5]

In addition, a 2019 SNL study[6] evaluated ten counterintelligence case studies to leverage lessons learned for insider threat within the nuclear industry based on conceptual and practical similarities. On a conceptual level, both counterintelligence and insider threat mitigation seek to protect high-value targets (critical information in the former and nuclear material in the latter) from human vulnerabilities. Both programs address potential threats to national security with serious consequences. In practice, both counterintelligence and insider threat mitigation involve preventive and protective mitigation efforts and are executed in a high security atmosphere.

The 2019 SNL counterintelligence case study analysis offered insights for insider threat practitioners based on trends in: position and level of authority, motivation, recruitment into intelligence collection, mechanisms for accessing sensitive information, maturity of reporting culture, preventive/protective measures, and investigative methods. This paper builds on the 2019 analysis by evaluating whether trends identified in the counterintelligence case studies are empirically present within the limited set of publicly available insider case studies in the nuclear field. This study finds that many of the trends in the counterintelligence dataset are reflected in the insider threat case studies, providing further evidence that counterintelligence offers useful insights for insider threat mitigation.

Counterintelligence Literature Review

While insider threat is a relatively nascent topic, the literature on counterintelligence reflects a long history of practice and evolution. The 1981 Executive Order 12333 provides the basis for modern U.S. federal government approaches to counterintelligence, defining counterintelligence as, "information gathered, and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations or persons, or international terrorist activities." This official U.S. policy is supplemented by a rich counterintelligence literature. For example, a 2001 Central Intelligence Agency (CIA) publication outlines best practices for counterintelligence professionals, including: be offensive, know your history, do not ignore analysis, do not be parochial, train your people, and never give up.[7] While similarities between these lessons and insights are observed in the insider threat literature,[8] they have not been explored in depth.

---

[2] Noah Pope and Christopher Hobbs, *Insider Threat Case Studies at Radiological and Nuclear Facilities*, Los Alamos National Laboratory, 2015, LA-UR-15-22642.

[3] Matthew Bunn and Kathryn Glynn, "Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries," *Journal of Nuclear Materials Management* 41, 3 (2013).

[4] Jarret M. Lafleur et. al., *The Perfect Heist: Recipes from Around the World*, Sandia National Laboratories, 2015, SAND2014-1790.

[5] Matthew Bunn and Scott D. Sagan, *A Worst Practices Guide to Insider Threats, Lessons from Past Mistakes* (Cambridge, Mass.: American Academy of Arts and Sciences, 2014).

[6] Noelle Camp and A.D. Williams, "Preliminary Results from a Comparative Analysis of Counterintelligence and Insider Threat in Nuclear Facilities," Proceedings Paper(s) for the *Institute for Nuclear Materials Management 60th Annual Meeting*, Palm Desert, CA, July 14-18, 2019.

[7] James M. Olson, "The Ten Commandments of Counterintelligence," *Studies in Intelligence*, 2001.

[8] Ibid.

Lessons learned from the literature on real-world espionage cases, including motivations for espionage, typical patterns of behavior and red flags, and examples of best (and worst) investigative practices can also be applied to the problem of insider threat. Drawing on the many publicly available cases, including firsthand accounts of espionage[9], works written by counterintelligence investigators[10], and comprehensive biographies[11], the Defense Personnel and Security Research Center (PERSEREC) has published several reports analyzing major trends in U.S. espionage. One recent report[12] analyzes demographic PERSEREC data to draw conclusions regarding acts of espionage, motivations, and consequences, while an additional report[13] suggests that characteristics of spies may be influenced by factors specific to the time period of the espionage. Evolving social and cultural factors may also impact the approach taken by insiders – for example, rapid technological development has led to nuclear industry concerns that an insider may take advantage of vulnerabilities in the cyber domain.[14]

Data, Methods, and Study Design

Evaluating individual case studies as the unit of measure, this research design is based on identifying trends across individual cases and comparing trends between datasets to elicit insights for insider threat mitigation. The ten case studies in "Dataset 1" were chosen in consultation with counterintelligence professionals to exhibit a range of counterintelligence lessons learned.[15] These case studies span a 60-year period between 1941 and 2001, representing a range of nationalities (German, Turkish, Swedish, American), and widely varied outcomes including successful prosecution, defection, and evading suspicion entirely. "Dataset 2" features seven insider threat case studies within nuclear and radiological facilities, drawn from the LANL/KCL study.[16] The objective of the case studies is to "illustrate that malicious acts by insiders have occurred" within nuclear and radiological facilities and provide detailed examples including profiles of perpetrators, incident timelines, and security system failures. The cases included in Dataset 1 and Dataset 2 are summarized in Table 1 below.

Table 1:

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	--	--

[9] Boris Morros, *My Ten Years as a Counterspy*, (New York: Dell Publishing Company, 1959).

[10] Scott W Carmichael, *True Believer: Inside the Investigation and Capture of Ana Montes, Cuba's Master Spy*, (Naval Institute Press, 2007).

[11] Ronald Kessler, *The Spy in the Russian Club*, (Pocket Books, 1992).

[12] Katherine L. Herbig and Martin F. Wiskoff, *Espionage Against the United States by U.S. Citizens 1947-2001*, Defense Personnel Research Center, Technical Report 02-5, (Monterey, CA, 2002).

[13] Katherine L. Herbig, Espionage by Americans: 1947-2007, Defense Personnel Research Center, Technical Report 08-05, (Monterey, CA, 2008).

[14] "'Cyber' & Insider Threats Among Targets of Nuclear Security Measures," International Atomic Energy Agency, 2004.

[15] Camp, Noelle, *Lessons Learned from Historical Counterintelligence Case Studies,* Sandia National Laboratories, June 2019, SAND2019-7265.

[16] Noah Pope and Christopher Hobbs, *Insider Threat Case Studies at Radiological and Nuclear Facilities*.

This paper conducts a comparative analysis within and across the two datasets to provide insight into whether trends identified in the counterintelligence case studies are empirically present within the limited set of nuclear facility-related insider case studies. The seven criteria in Table 2 were devised as a rubric for analyzing insights from the case studies with implications for insider threat mitigation.

Table 2:

Element Elicited from the Case Studies	Implications for Insider Threat Mitigation
Position/title of individual	Provides insight into the role of organizational position, access, authority, and status on insider threat potential
Motivation(s)	Provides insight into motivations attributed to insiders in international best practice documents
Recruitment/transition into intelligence collection*[17]	Provides insight into potential indicators of *individual* susceptibility for engaging in malicious acts
Mechanisms for accessing sensitive information	Provides insight into role of level of access on insider threat potential
Maturity of the "reporting culture"	Provides insight into role of *operational environment* susceptibility to manipulation for malicious acts
Impact of "preventive" & "protective" measures	Provides insight into insider threat potential by mapping to traditional, high level insider threat mitigation functions
Impact of investigative measures	Provides insight into potential insider response mechanisms

The following detailed summary[18] of the case of former U.S. Navy photographer and Russian spy Glenn Michael Souther (featured in Dataset 1) provides an example of how the seven-criteria rubric was applied to each case. Souther was recruited as a spy for the Soviet Union in 1980 while serving as a U.S. Navy photographer in Italy with relatively limited access to classified information. By 1984, however, Souther was working as a Naval reservist at the Top Secret Navy facility FICEURLANT. Souther's case demonstrates that insiders may use promotions or lateral moves to increase opportunity for malicious action. Souther's espionage was motivated by a combination of disgruntlement, ideological sympathies, and money. Souther complained to friends and family about the poor treatment of enlisted Navy personnel and was ideologically drawn to the Soviet Union, once telling a girlfriend that "Communism is the perfect form of government." He supplemented his reservist salary with money provided by Soviet intelligence, gifting friends and family expensive items.

Souther obtained much of the information he compromised over the course of his regular duties at FICEURLANT. He also took advantage of lax security measures at the facility to access material not directly related to his work. As no record was kept of the comings and goings of employees, Souther came to work at unusual times when his espionage was less likely to be noticed. More robust security procedures, including monitoring and a two-person rule to prevent a single individual from accessing highly classified material alone, could have benefited the facility. The Souther case also demonstrates how poor reporting culture can enable malicious activity. None of Souther's colleagues across nearly a decade of Naval service ever reported inappropriate behavior, including multiple indicators of espionage such as unusual work hours, undue affluence, criminal behavior, and suspicious foreign travel.

Souther's case demonstrates both the necessity of thorough and complete background investigations and the importance of not relying on a single measure for insider threat mitigation. His criminal record (including a conviction for sexual battery), unpredictable outbursts, and vocal anti-U.S. political views should have raised red flags for his clearance adjudicators. Yet when interviewed by

[17] For the insider threat case studies, this criterion is expressed as "decision for action(s)."

[18] For more details, please see: Camp, Noelle, *Lessons Learned from Historical Counterintelligence Case Studies,* Sandia National Laboratories, June 2019, SAND2019-7265.

investigators in 1983, Souther's girlfriend noted that it "seemed more like a five-minute job interview for a job at Kmart" than for a Top Secret clearance. The investigative process in the Souther case was poorly managed, including discounting reports from Souther's ex-wife about the espionage in 1982 and failing to gather evidence in advance of a 1986 interview to elicit a confession. Alerted by the interview to investigators' suspicions, Souther defected to the Soviet Union, where he lived until his death by suicide three years later.

Results

As modeled by the Souther case study summarized above, the seven-criteria rubric was applied to both datasets to elicit lessons learned for insider threat mitigation. The rubric criteria were selected to provide insight into insider characteristics, typical patterns of insider behavior and red flags, and the effectiveness of mitigation and investigative measures. The same criteria were applied to both datasets, with the exception of "recruitment/transition into intelligence collection," which is expressed in Dataset 2 as "decision for action." Analysis of the ten counterintelligence and seven insider threat case studies reveals several patterns that may provide useful lessons for insider threat mitigation techniques.

Dataset 1: Counterintelligence Case Studies

Summarizing the results of the 2019 SNL paper,[19] several key trends emerge. For example, the type of position and level of authority varied widely in Dataset 1, ranging from CIA clerk Sharon Scranage (low authority) to DIA senior analyst Ana Montes (high authority). In addition, the majority (7/10) of cases in Dataset 1 were motivated by financial gain. While spies in the dataset received outside direction and assistance over the course of their espionage, most spies made the initial decision to volunteer on an individual basis. In several cases, the decision to volunteer was preceded by a "trigger event" in the individual's personal life, such as divorce in the cases of Aldrich Ames and Jim Nicholson. While in seven of ten cases compromised information was accessed over the course of normal duties, in the cases of Ana Montes, Jim Nicholson, and Elyesa Bazna, the spies sought to expand their access to classified information. Efforts to expand access were risky, however, drawing the attention of coworkers and investigators. Reporting culture in most cases was underdeveloped, allowing spies to continue their espionage undetected for longer. Unsurprisingly, two of the three cases that included a strong reporting culture resulted in favorable outcomes for the investigation, including successful prosecution. Failure patterns in hiring practices, such as background investigations (4/10), and security failures, including poor storage of classified information (4/10), were also observed. In the case studies examined, each investigation proceeded uniquely, leveraging diverse methods including double-agent operations, clandestine intelligence, face-to-face interviews and polygraph examinations. Electronic and/or physical surveillance measures were among the most popular investigative measures, employed successfully in 5/10 cases. For a more detailed summary, please see Table 4 in the 2019 SNL paper.[20]

Dataset 2: Insider Case Studies

<u>Position/Title of the Individual</u>

Type of position and level of authority varied within the dataset, ranging from facility director to technician. In one instance, collaborating insiders including the Director of Stable Isotope Production, Deputy Head of Finance, and a mix of engineers, chemists, and technicians, combined knowledge and

[19] Noelle Camp and A.D. Williams, "Preliminary Results from a Comparative Analysis of Counterintelligence and Insider Threat in Nuclear Facilities."
[20] Ibid., 10.

expertise from multiple areas to more effectively exploit facility vulnerabilities. Of note, two of the seven cases in the dataset involved workers in temporary contractor positions. Rodney Wilkinson first stole the blueprints for the South African Koeberg Nuclear Power Station while employed as a contractor and later returned to the facility in a second temporary position to carry out the sabotage. David Learned Dale, a temporary employee of a facility subcontractor at GE Nuclear Power Plant in North Carolina, stole uranium oxide power only a few months before his job was due to expire. His brother later claimed that Dale was "depressed" by the prospect of his job ending.

Motivations

Five of the seven cases in the dataset were motivated to commit insider activity by financial considerations. Of these cases, three were impacted by the economic impacts associated with the fall of the Soviet Union. Several of the financially motivated insiders had modest financial ambitions – Leonid Smirnov, for example, wanted to "buy a new stove and refrigerator," while David Learned Dale hoped to "take his girlfriend out to dinner." Other motivators included ideology and possible disgruntlement.

Decision for Action

As previously mentioned, three cases were "triggered" by economic difficulties associated with the fall of the Soviet Union. Two cases involved possible or confirmed ties to outside organizations. Rodney Wilkinson brought blueprints of the Koeberg plant to the African National Congress, who then encouraged and trained Wilkinson himself to carry out the sabotage. Additionally, sabotage of the Doel plant in Belgium may be linked to an Islamic extremist organization. While the perpetrator of the Doel sabotage has never been identified, video footage of another Belgian nuclear facility was found in the apartment of a suspected militant linked to terrorist attacks in Paris.

Mechanisms for Accessing Material

The majority of cases demonstrated insiders taking advantage of access directly associated with their daily role within the facility. Leonid Smirnov used his authorized access to highly enriched uranium dioxide to divert small quantities of nuclear material while colleagues were out of the room. Multiple cooperative insiders at the Elektrokhimpribor facility in Russia, including the Director of Stable Isotope Production, diverted 5-10% of isotope solution and diluted the solution with distilled water to avoid detection. Conversely, the case of David Learned Dale provides an example of an insider gaining unauthorized access to sensitive material. Hired into a temporary subcontractor position, Dale worked the day shift at the Chemical Technician Lab but did not have access to the adjacent uranium store building. On January 26, 1979, Dale entered the plant with the night shift and penetrated the plant's security system by: exploiting known access control flaws, entering the uranium store via an unlocked door, transporting two cans of uranium dioxide to the Chem Tech Lab where he worked, removing some of the nuclear material, and storing it in the trunk of his car.

Maturity of the "Reporting Culture"

No cases in Dataset 2 exhibited a strong reporting culture. In two of the cases, individuals within the facility were aware of the malicious activity but did not report due to coercion or rationalization of the insider actions. In the Elektrokhimpribor case plant workers justified their colleagues' actions by claiming "there was no other way … to make money." In two additional cases, colleagues failed to report suspicious indicators including drunkenness in the workplace and accessing restricted areas.

Impact of "Preventive" and "Protective" Measures

The most common preventive and protective failures included failure of access control (3/7), failure of materials accounting practices (2/7), and failure to employ a two-person rule (2/7). Failure of

access control likely occurred in both sabotage cases, as well as the case of theft involving unauthorized access. In these three examples, insiders took advantage of facility vulnerabilities such as unlocked doors and an unsecured ventilation system to carry out malicious acts. More effective materials accounting practices would also have proved useful in several cases involving diversion of small amounts of nuclear material. Additionally, lack of a two-person rule enabled insiders such as Leonid Smirnov to engage in malicious activity undetected by coworkers.

The case of Alex Maestas at Los Alamos Plutonium Facility provides a rare example of successful implementation of protective measures. While attempting to leave the facility with a 50-gram piece of gold contaminated with plutonium, Maestas set off a radiation portal monitor designed to detect beta and gamma radiation. Maestas was unable to adequately explain his possession of the gold and was subsequently detained by Department of Energy personnel until authorities could arrive. In this case, the radiation portal monitor successfully identified the diversion of nuclear material, and security personnel at Los Alamos acted appropriately to recover the material and apprehend the insider.

Impact of Investigative Measures

Successful investigations employed a variety of techniques to identify the insider and reclaim missing material. Investigators first became suspicious of the multiple collaborating insiders in the Elektrokhimpribor case when they noticed extravagant displays of wealth (including houses and cars) anomalous to the region and inconsistent with salaries paid by the facility. In another successful investigation, customs officials reported discrepancies between the stated and actual radiation levels of shipments from Radioisotope Factor No. 45 at Mayak Production Association in Rusisia. Not all investigations within the dataset were successful – in the case of sabotage at Doel 4 Nuclear Power Plant, the perpetrator remains unknown. In the case of Leonid Smirnov, the facility had no knowledge of missing material and Smirnov was arrested in a chance encounter involving stolen batteries.

The results of Dataset 2 analysis are summarized in Table 3 below.

Analysis

Analysis of Dataset 1 and Dataset 2 demonstrates that many of the trends in the counterintelligence dataset are also reflected in the insider threat case studies.

Position/Title of Individual

In both datasets, position and authority varied widely. Both Dataset 1 and Dataset 2 included cases in which spies or insiders took advantage of high authority to conduct malicious acts. Individuals with high levels of authority in both datasets leveraged their authority as a key component of their strategy. For example, A. Kalinovsky (KCL5) used his position as director to coerce subordinates into collaboration and DIA senior analyst Ana Montes (SNL1) used her contacts and reputation to expand her access. Both datasets also included individuals with very low authority. In these cases, it is possible that the individuals' suspicious activity went unnoticed in part due to their low organizational status. CIA clerk Sharon Scranage (SNL3) transcribed the contents of sensitive cables that passed across her desk, while Safety Officer Rodney Wilkinson (KCL4) smuggled mines into the facility without detection.

Both datasets also included a single example of multiple collaborating spies/insiders at different levels of the organizational hierarchy working together (SNL4 and KCL3). Clyde Conrad, an Army Noncommissioned Officer, purposefully recruited vulnerable junior enlisted service members to join his spy ring. The Director of Stable Isotope Production at Elektrokhimpribor facility devised a scheme to divert isotope solution to sell for profit, recruiting eight other employees from across the facility including engineers, chemists, technicians, and finance officers. In these cases, varied access, authority, and knowledge was an asset to the group.

Table 3:

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[21]
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)[22]	Possible tie to Islamic extremist organization[23]	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

[21] A "successful" investigation in this context entails only that the individual was identified, arrested, and prosecuted. It is important to note that many of the investigations identified as successful may also have experienced setbacks and delays or suffered from mismanagement.

[22] Alissa J. Rubin and Milan Schreuer, "Belgium Fears Nuclear Power Plants are Vulnerable," The New York Times, 25 March 2016.

[23] Ibid.

In Dataset 2, two cases included a temporary contractor (KCL2 and KCL4). The temporary nature of the work likely shaped the timeline of the malicious activity in both cases and may have served as a motivation for theft in the case of David Learned Dale (KCL2). This trend is not present in Dataset 1, as all the cases are long-term employees.

Motivations

In both datasets, financial motivation was most common. In Dataset 1, spies often used the money gained from espionage to make lavish purchases such as a new house and car (SNL6) and plane tickets and luxury goods (SNL2). This was also true in the Dataset 2 Elektrokhimpribor case (KCL3), in which investigators identified the perpetrators based on purchases inconsistent with their income level. However, in Dataset 2 several insiders also exhibited less conspicuous financial motivations such as buying essential household appliances (KCl1) or taking a significant other out to dinner (KCL2). This trend suggests that insiders may be willing to commit a malicious act for relatively modest financial ambitions that may fall outside the realm of detectable undue affluence.

Other motivations across both datasets were diverse, including ideology (SNL1 and KCL4) and disgruntlement (SNL9, SNL10, KCL6). Dataset 1 also featured two examples of blackmail (SNL6 and SNL8) and four examples of ego (SNL3, SNL7, SNL9, SNL10).

Recruitment/Decision for Action

While spies in Dataset 1 received outside direction and assistance over the course of their espionage, most spies made the initial decision to volunteer on an individual basis. Likewise, most of the cases in Dataset 2 were internally motivated, with a few cases of insiders working with an outside organization (KCL4 and possibly KCL6). Both datasets included examples of major life events as "triggers." In three cases in Dataset 1, espionage was preceded financial and emotional turmoil, including denied promotion (SNL10) and divorce (SNL5 and SNL6). In Dataset 2, insider activity occurred after reduction of salary (KCL1, KCL3, KCL5) and notification of end of contract (KCL2).

The role of "trigger events" in both datasets has several potential implications for insider threat mitigation. First, the presence of "trigger events" suggests that events in an individual's personal life may affect the decisions he or she makes in the workplace. Offering employee assistance programs such as counseling may help employees grapple with emotional distress without turning to insider activity. Additionally, major events in the workplace including reduction of salary, denied promotion, and end of contract may foster disgruntlement that ultimately leads to insider activity. Consistent with other insider studies[24], this trend suggests that organizations should observe employees receiving potentially disappointing news for warning signs of growing disgruntlement or revenge.

Mechanisms for Accessing Material/Information

The majority of insiders and spies used their normal, everyday access to information and nuclear material to facilitate espionage and insider activity, suggesting that both spies and insiders typically take advantage of what they already have access to in order to commit malicious acts. This insight has important implications for insider threat mitigation, as many security programs focus on identifying insiders through tracking anomalous behavior. The approach of tracking anomalies is likely insufficient to identify insiders whose malicious acts are camouflaged by their ordinary responsibilities.

In some cases (SNL5, SNL7, SNL10), spies attempted to gather information outside their direct need to know, primarily through asking other employees to provide it as a favor. Expanding access beyond their established "need-to-know," however, was risky, often raising the suspicions of coworkers.

---

[24] Daniel J. Pond, et. al, *Enhanced Security through Human Error Reduction: Factors Contributing to Errors and Breaches*, Los Alamos National Laboratory, 2002, LA-UR-02-0815.

In one case of espionage (SNL2) and one case of insider theft (KCL2), the individual physically broke into a restricted area to obtain information or material. In both these two cases of unauthorized access, 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, with no successful examples of reporting culture in Dataset 2. In Dataset 1, successful reporting culture generally resulted in positive outcomes for the investigation (SNL1 and SNL5). These results demonstrate that nuclear facilities could potentially benefit from more robust facility-wide training on insider threat and a user-friendly system to report insider incidents. The benefits of reporting, however, were only realized if security professionals appropriately followed up. As summarized in the in-depth case study above, Glenn Michael Souther's ex-wife reported his espionage to Navy officials in 1982 but was not taken seriously by investigators. As a result, Souther continued to spy for an additional three years before his defection to the Soviet Union.

Impact of "Preventive" and "Protective" Measures

Failures of background investigations occurred in both datasets. Investigations frequently failed to identify red flags present in an individual's background prior to hiring or during the reinvestigation period. In Dataset 1, background investigations failed to uncover a host of issues including past drug use (SNL1, SNL4, and SNL6), falsified education (SNL1), anti-U.S. views (SNL1, SNL2) and criminal history (SNL2, SNL7). In Dataset 2, it is unclear how many of the insiders received an initial/subsequent (re)investigation. In at least one case (KCL4), a background investigation was never administered.

Both datasets also exhibited failures of protective measures. In Dataset 2, this often manifested as a failure of physical security, including failures of the physical protection system and access control system (KCL2 and KCL4 respectively). In Dataset 1, security failures typically related to the storage of information, either through lapses in physical storage mechanisms for classified information (SNL4) or information security practices such as compartmentation (SNL1).

Impact of Investigative Measures

Means of investigation varied widely across both datasets. In Dataset 1, physical and electronic surveillance was commonly used to gather evidence. In Dataset 2, there was insufficient data to identify trends, but portal monitors (KCL7) and customs enforcement (KCL5) were used successfully in one-off cases. The diversity of approaches and outcomes made it difficult to discern useful patterns during analysis. How and when to implement various investigative techniques for insider threat mitigation requires additional analysis for appropriateness and practicality.

Conclusions

Comparing insights from counterintelligence and insider threat case studies demonstrates that counterintelligence represents a useful corollary to insider threat mitigation in nuclear facilities. Many of the same trends appeared across both the counterintelligence and insider threat datasets, including a range of authority levels, primarily financial motivations, the presence of "trigger events," use of normal, everyday access to facilitate malicious activity, and failures of background investigations and security measures. These findings suggest that 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. Further, the practice of the counterintelligence discipline may provide useful lessons for nuclear security practitioners, particularly in the areas of cultivating reporting culture and improving insider threat investigations.