

MAXIMIZING PERSONNEL SECURITY TO MINIMIZE THE INSIDER THREAT

Molly Rickard, Michael Majewski, Lindsay Odell and Ben Perman, Booz Allen Hamilton, Inc. Washington, DC

INSIDER THREATS ARE NOT LIMITED TO SELECT AGENT LABORATORIES. All life science and medical institutions can be potential targets of insider threat. Insiders with access to valuable biological material pose the single greatest threat to the science community because they have the ability to bypass many internal biosecurity measures. It is important to note that often there are behavioral indicators to identify such individuals before they commit a criminal act.

INTRODUCTION

With the growing interest in mitigating insider threats, laboratories are recognizing the need to take proactive measures to ensure their facilities and staff operate in a secure manner. Entities that house Tier 1 select agents are now required under the Select Agent Regulations to implement pre-access suitability and ongoing suitability (reliability) measures in an effort to prevent insider threats. The new Select Agent Regulations, however, do not specifically describe how to implement a comprehensive personnel security program, which goes beyond suitability and reliability concepts. In the absence of specific guidance, laboratories and biomedical institutions are challenged to effectively implement comprehensive security practices that address the insider threat.

METHODS

Our methods are adapted from the Exceptional Case Study Program (ECSP), initially a U.S. Secret Service study of known “attacks on principal” that identified and analyzed 83 persons known to have engaged in 73 incidents of assassination, attack, and near-attack behaviors from 1949 to 1995. The ECSP did not focus on threats that are immediately relevant to biosecurity concerns. We have turned to a group of case studies focused mainly on threats to the biomedical and microbiological research community, clinical and veterinary medicine and other public health institutions. The criteria used for selecting cases studies were as follows:

- The threat operated in or against the three communities of interest.
- The cases are adjudicated.

THE INSIDER THREAT—IS IT REAL?

All life science and medical institutions can be potential targets of insider threat. These institutions contain biological materials and technologies, as well as employees that have unique knowledge and access, which adversaries might seek to misuse. Cases of targeted violence or insider threat within the workplace or school settings have been well documented, and include cases that involve laboratories and scientists [see Table 1]. Within the science community, the threat may encompass a broad range of scenarios, such as data falsification or manipulation, research sabotage or espionage, and unapproved experimentation, to more serious incidents of theft or violence. Insiders with access to valuable biological material pose the single greatest threat to the science community because they have the ability to bypass many internal biosecurity measures. It is important to note that often there are behavioral indicators to identify such individuals before they commit a criminal act. The perpetrator does not “just snap” without giving away certain behavioral indicators.

WHY CARE ABOUT INSIDER THREAT AND BIOSECURITY?

The impact of a bioterrorism event is potentially very high, costing both lives and infrastructure. The anthrax letters mailed during October 2001 resulted in 5 deaths, decontamination costs totaled about \$320 million, and there was significant public fear for several weeks after the attacks. There can also be impact to the scientific community as a result of any future biological events. Post-attack repercussions might include the loss autonomy in managing entity biosecurity measures, greater governmental research oversight, and additional (potentially costly) security requirements. Even incidents which do not result in bioterrorism can still have the potential to do serious harm to a scientific/medical institution. Insider threats can commit criminal/violent acts, or damage the credibility or integrity of an institution. Therefore, there is a vested benefit to scientists to proactively implement a safe and secure culture to protect their laboratory and program integrity.

PERSONNEL SECURITY PROGRAMS ARE KEY TO INSIDER THREAT DETECTION

Personnel security is comprised of measures that focus on human behavior, rather than physical vulnerabilities, to counter the unique challenges posed by insider threats. There are four components of a personnel security program that provide an institution and its personnel with the capability to effectively detect, monitor, address, and protect against the insider [see Figure 1]. These measures can be used by all institutions (including non-select agent entities) to counter a wide range of insider threats. Key components of personnel security include:

- Pre-access Suitability**—seeks to determine if an individual is suitable for access to valuable biological materials and establishes a behavioral baseline that can be used to compare significant behavioral changes.
- Ongoing Personnel Reliability**—allows for ongoing assessment to identify if/when an individual deviates from their behavioral baseline and is based on strong peer and self reporting programs.
- Personal Security**—protects individuals from unknowingly colluding with an insider threat and in their daily lives outside of work by educating them in areas such as operation security, information security, and threat awareness, including elicitation, manipulation and deception awareness.
- Training**—an important but often overlooked component of personnel security that educates staff and management how to effectively promote and conduct suitability, reliability, and personal security measures.

THREAT (PERSON)	INCIDENT	POTENTIAL PREVENTATIVE/MITIGATION MEASURES
 Diane Thompson	1996. Disgruntled lab technician at St. Paul Medical Center in Dallas, TX; infected 12 co-workers with Shigella dysenteriae via pastries in office break room. Was not her first offense; in 1995 she gave tainted food to boyfriend; fabricated his lab reports to prevent correct diagnosis. Used contaminated syringe to take a sample of boyfriend's blood. Several additional violent acts, mainly targeted at boyfriend.	PRE-ACCESS SUITABILITY: Thorough background check or interview with peers would have identified a history of violence or odd/controlling behavior. ONGOING PERSONNEL RELIABILITY: Occupational Health & Wellness—would have provided a venue to discuss grievances with coworkers.
 Gang Lu	1999. Physics/astronomy student who received PhD from University of Iowa. Killed 5 after failing to win a dissertation prize. Isolated loner who did not like to interact with other students. Didn't like being challenged, reported to have had abusive tantrums. Purchased a gun, practiced shooting. Sent sister in China \$20K shortly before shooting. Wrote 5 letters explaining his grievances; letters intended to be mailed to media outlets.	ONGOING PERSONNEL RELIABILITY: Abusive tantrums not reported by roommates or colleagues. Lu appeared in person twice to complain to the Associate Vice President of Research, however did not lead to any significant action to mitigate his grievance, which might have prevented the attack.
 Eric Robert Rudolph	1990s. Responsible for series of bombings that killed 2 and injured over 150; in name of anti-abortion and anti-gay agenda. Used elicitation techniques including flattery to bribe young female temporary employees and new admin at clinics to obtain info. Successfully infiltrated security, admin, and scheduling of clinics. Dated multiple receptionists, knew security guards on first name basis.	PERSONAL SECURITY: Staff unaware of basic elicitation and manipulation tactics, which ultimately provided Rudolph access and information that helped him attack the clinics.
 Bruce Ivins	2001. Anthrax researcher at USAMRIID; responsible for vaccine development. Primary suspect in Amerithrax case involving highly refined <i>Bacillus anthracis</i> ; estimated 47 letters mailed; 4 recovered. Resulted in 22 infections that led to 5 deaths. Significant history of behavioral and psychological disturbance, including criminal offenses. Stalking behaviors also exhibited at USAMRIID with two female employees, (one woman was told by management to go into hot lab where Ivins couldn't bother her). Ivins had requested to remove himself from lab but lab management refused.	PRE-ACCESS SUITABILITY: Ivins' past contains several indicators: he vandalized a neighbor's house as a juvenile; carried and discharged a firearm while a student and was involved in a life-long obsession with a sorority and its members for which he used false identities and deception to provide cover for various illicit/clandestine activities. ONGOING PERSONNEL RELIABILITY: Co-workers' concerns about Ivins' behavior were reported but not acted on by the Command, at the same time other coworkers, aware of Ivins' persecutory beliefs, discussions about poisoning, and stalking behaviors, often failed to report. Ivins shared plans to poison with coworkers. PERSONAL SECURITY: Repeatedly used elicitation and manipulation techniques with female stalking targets. Used gifts to elicit sympathy and favors (quid pro quo).
 Seung-Hui Cho	2007. Undergrad student who killed 32, wounded 25 at VA Tech. Massacre highlighted gaps in gun control laws, since Cho has been adjudicated by court as risk to self and others. Cho repeatedly expressed angry and violent depictions in school writing assignments. Concerns were filed to school admin. Law enforcement was aware of stalking incidents. However, law enforcement and school admin did not communicate different but relevant concerns.	PRE-ACCESS SUITABILITY: After a stalking report, a VA court found that Cho was “an imminent threat and issued a detention order. Police still allowed Cho to purchase weapons because the detention order was not shared with the Federal databases that are used for firearms records checks under the Brady Act. ONGOING PERSONNEL RELIABILITY: Teachers and students had significant concerns over Cho, but some never reported their concerns, other concerns were reported but not addressed in effective manner. Reports included suicidal ideation and intimidating poetry. School admin, security, and mental health professionals did not effectively share information with each other so all ‘pieces of the puzzle’ were not seen.
 Mohsen Hosseinkhani	2009. Mt. Sinai Researcher that lost fellowship because his work was “not up to snuff.” After being fired, broke into lab—twice—to steal research equipment (~\$10K) and sabotaged experiments. Later determined that original background information he provided was not credible (not found in university registries, resident address was not accurate). Hosseinkhani fled to Iran to avoid prosecution despite his passport having been seized by the court.	PRE-ACCESS SUITABILITY: Thorough background check would have identified gaps/inaccuracies in resume and personal information. Hosseinkhani had an incomplete MD and PhD from two medical schools and provided a false home address. TRAINING: Better termination practices by Lab Security—immediate removal of access to laboratory should occur once termination procedures are implemented to prevent post-termination sabotage.
 Amy Bishop	2009. Killed 3, wounded 3 after being denied tenure in Biology Dept. at University of Alabama. History of violence (accidentally killed brother; unrelated violent attack at restaurant). Multiple colleagues expressed her behavior as abrasive, narcissistic, bizarre, and out of touch with reality. Several students signed a petition and sent to Department head, however did not result in classroom changes.	PRE-ACCESS SUITABILITY: Thorough background check might have identified history of violence and potential murder. Interviews with past coworkers might have revealed consistent pattern of abusive behavior. ONGOING PERSONNEL RELIABILITY: Colleagues had concerns over her “bizarre tangents” and being “crazy” but did not report concerns. Management did not conduct Threat Assessment when received student petition arguing concerns over Bishops “ineffective” teaching ability and “odd, unsettling ways.”

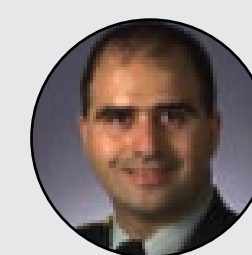
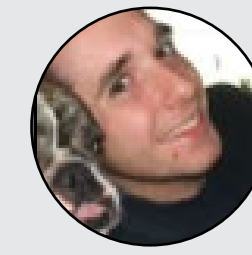
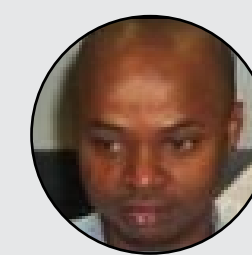

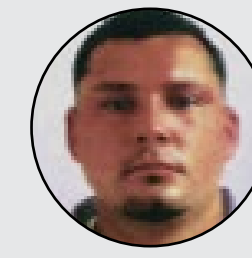
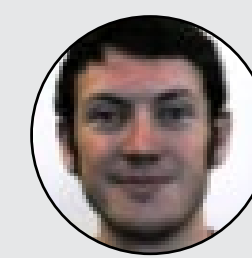
THREAT (PERSON)	INCIDENT	POTENTIAL PREVENTATIVE/MITIGATION MEASURES
 Nidal Malik Hasan	2009. Army psychiatrist; killed 13 and wounded 29 others. Worked at Walter Reed Medical Center. Before being transferred to Fort Hood, received a poor performance evaluation. Colleagues and superiors at Walter Reed were deeply concerned about his inappropriate behavior and comments. Described him as disconnected, aloof, paranoid, and belligerent (but never reported). Unsuccessfully attempted to contact Al Queada to collaborate.	PRE-ACCESS SUITABILITY: Hasan had received a negative evaluation upon departure from Walter Reed just prior to a scheduled deployment. ONGOING PERSONNEL RELIABILITY: Colleagues at Walter Reed Army Hospital were aware of Hasan's behavior and potential indicators of violence but assumed that in a clinical psychiatric setting others would report (diffusion of responsibility). Hasan made “outlandish” comments about the U.S. presence in Iraq and Afghanistan and the obligation of Muslim soldiers to fight the oppressor (U.S.). Hasan's family members knew of attempts to separate from the Army prior to an upcoming deployment to Afghanistan.
 Raymond Clark	2009. Vet lab tech at Yale murdered graduate student Annie Le. Clark complained about Yale researchers not following animal husbandry protocols; had emailed Le criticizing her protocols. Clark had previously demonstrated aggressive behavior and violent propensity towards women; had displayed controlling behavior. Clark arrested based on DNA, facility keycard, and video surveillance.	PRE-ACCESS SUITABILITY: Reference interviews might have revealed consistent pattern of aggressive, controlling behavior towards women. PERSONAL SECURITY: Le was working alone the day attacked and killed.
 Konan Michel Yao	2009. Researcher studying Ebola virus and HIV vaccines. Hired by Canadian Public Health Agency to work as PhD fellow in lab. Was to begin new job at NIH biodefense facility in MD; Stole 22 vials containing DNA encoding specific Ebola genes on last day of work at Canadian lab. Wanted to take vials to new job so wouldn't have to start research from scratch. Yao had signed a form that declared he did not steal anything from the lab. Lab Security Director: “This individual had secret security clearance and we relied on his integrity.”	TRAINING: Better termination practices by Lab Security—check employee stocks to ensure nothing missing or conduct termination interview; potentially could have identified suspicious behavior if asked Yao if planned to take research with him. Better training in acceptable shipping practices, such as legal methods for mailing biological hazards if obtained permission from host Lab; if Yao had known of such practices, might not have illegally taken his vials in secret in his car.
 Vipul Bhrigu	2009. Meticulously and systematically sabotaged work of lab colleague, Heather Ames, over 3 month period. Tampered with her experiments and poisoned her cell-culture media with alcohol in attempt to slow down her work so that he could “breathe” in the big pond. When Ames first reported suspicions to lab manager, she was not taken seriously and originally target of investigation. After cameras installed in lab, Bhrigu found guilty of sabotage.	PRE-ACCESS SUITABILITY: Bhrigu lied about his dismissal from Michigan and violated his parole by traveling to India, was hired by his alma mater, University of Toledo. Toledo should have contacted peer or co-worker references. ONGOING PERSONNEL RELIABILITY: Initial peer reports were regarded as paranoia by peers and advisors, led to a University of Michigan Police criminal investigation of Ames, not Bhrigu (reprisal).
 David Kwiatkowski	2012. Radiological technician accused of infecting 31 hospital patients with Hepatitis C by stealing fentanyl syringes and replacing them with dirty ones tainted with his blood. Co-workers reported him acting strangely. Worked in 10 hospitals over 4 years in eight different states; several misconduct and disciplinary incidents but derogatory info never reported to HR or supervisors at new jobs; hiring institutions didn't follow-up on references or gaps in work history.	PRE-ACCESS SUITABILITY: Clinics that hired Kwiatkowski should have looked into the circumstances of his dismissal from prior employers, contacted co-workers or peers, and inquired about gaps in work history. ONGOING PERSONNEL RELIABILITY: Peers noticed strange behavior and should have reported it, supervisors should have documented reports and acted to remove Kwiatkowski from his position.
 James Holmes	2012. Killed 12 and injured 58 others in movie theater massacre. Neuroscience Graduate student at University of Colorado, withdrew after qualifying exams. Conducted surveillance/planning 6+ months before attack. Psychiatrist treating Holmes reported concerns to police and campus threat assessment committee; but no action taken because Holmes withdrew. Holmes texted another student asking about mental disorders and warned student to stay away from him.	PRE-ACCESS SUITABILITY: Holmes had a history of violence and mental health treatment. His mentor during an internship at the Saulk Institute described him as “stubborn, uncommunicative and inept.” In contrast grad school recommendation letters called him an “effective group leader.” ONGOING PERSONNEL RELIABILITY: Psychiatrist reported concerns over behaviors to campus police and Threat Assessment Team. Both organizations failed to respond or refer the case to local authorities when Holmes withdrew even though his departure could have been a key indicator of the pending attacks. Holmes sent text messages to an associate warning her to stay away from him. The operator of a small arms range warned employees about Holmes because of his “bizarre” voice mail message.

TABLE 1: THREAT CASE STUDIES. This table demonstrates that the science community is not immune to the insider threat. There are dangerous individuals within the scientific community (like any sector) and that nefarious acts have occurred within the laboratory setting. The table also highlights that often the threat is detectable prior to the act of violence (i.e. the perpetrator does not “just snap” one day), as seen by the listed potential preventative/mitigation measures.

CONCLUSION

- The insider threat is real but detectable.
- Implementing personnel security is in the best interest of scientific entities.
- Key components of a personnel security program are:
 - Pre-access Suitability
 - Ongoing Personnel Reliability
 - Personal Security
 - Training (for both staff and management)

RESOURCES

- Arizona State University: Personnel Suitability Program for Tier 1 Biological Select Agents and Toxins. ASU Department of Environmental Health and Safety. (2013). www.asu.edu/ehs/documents/asu-personnel-suitability-plan.pdf
- CDC Guidance for Suitability Assessments. http://www.selectagents.gov/resources/Tier_1_Suitability_Guidance_v3-English.pdf
- CDC Suitability Plan Template. http://www.selectagents.gov/resources/Suitability_Template_Final_APHIS-CDC-English.pdf
- Developing a Behavioral Health Screening Program for BSL-4 Laboratory Works at the National Insititutis of Health. Skvorc and Wilson (2011) Bisecur Bioterr 9: 23–29. <http://www.ncbi.nlm.nih.gov/pmc/articles/PMC3063697/>
- Report of the Virginia Tech Review Panel (2007). <http://www.governor.virginia.gov/tempcontent/techpanelreport.cfm>
- Report of the Experts Behavioral Analysis Panel (REDACTED). Saathoff et al. 2011. https://www.researchstrategiesnetwork.org/images/docs/Document_Interior_062711_Redacted.pdf
- Research Strategies Network Evaluating Risk for Targeted Violence in Schools: Comparing Risk Assessment, Threat Assessment, and Other Approaches (2001). http://www.secretservice.gov/ntac/ntac_threat_postpress.pdf
- Protective Intelligence and Threat Assessment Investigations. Fein and Vossekuil. 1998 National Institute of Justice. http://www.secretservice.gov/ntac/PI_Guide.pdf
- Total Decontamination Cost of the Anthrax Letter Attacks. Schmitt and Zaccia. (2012). Bisecur Bioterr 10:98-107.
- Assassination in the United States: An Operational Study of Recent Assassins, Attackers, and Near-Lethal Approachers. (1999). Fein and Vossekuil. Journal of Forensic Sciences. http://www.secretservice.gov/ntac/ntac_ifs.pdf

