Book Review

Mark L. Maiello, PhD
Book Review Editor

Insider Threats

Edited by Mathew Bunn and Scott Sagan
Softcover, 181 pages
ISBN 978-1-5017-0516-8
Cornell University Press, Ithaca and London, 2016

Can the insider threat experience of non-nuclear industries and incidents inform the insider threat planning of nuclear security operations? The contention of editors Bunn and Sagan is yes. Their effort is to do so is this short treatise written with seven other experts. This interesting take on the subject was motivated — until now — by the lack of information and data on the subject within the nuclear industry. The editors have looked to the casino and pharmaceutical industries and well-known incidents such as the anthrax mailing attacks of 2001, in addition to insider attacks at military bases, to get out ahead of a nuclear insider threat incident.

The editors performed unprecedented research into the problem area. The results indicate that there have been many incidents of insider threats at nuclear facilities, but few linked to terrorists. The paucity of *jihadi* interest — as measured by Internet forum activity and other research — further diminishes the probability of a terrorist threat. Even when terrorists consider a nuclear target, assault rather than infiltration appears to be their choice. From 1970 to 2012, of the 113,000 terrorist events recorded, only 58 involved nuclear targets — and of those, only four involved an insider. Yet Bunn and Sagan pressed on to produce this book, indicating that the threat — if ever carried out — is simply too dangerous to ignore.

Insiders are personnel within government, military, academic, and private-sector facilities with access to potentially dangerous information, procedures, or hazardous materials. They obviously need not be or be affiliated with terrorists. A grudge, an exaggerated sense of unfair treatment, mental imbalance, or other factors may push a disgruntled employee to take actions that endanger colleagues and/or the public. And herein lies another concern: according to the editors, the insider threat is viewed with some complacency by most employers. Pre-employment vetting by background checks is frequently viewed as adequate but is, of course, dependent on the depth of the investigation process. It also fails to take into account the time-dynamics of human nature: people and their circumstances change. They have normal human failings and they sometimes suffer unfortunate changes to their work life and in their relationships. They are subject to illness, aging, personal loss, and grief. Will some cross the line into dangerous behavior if they undergo these misfortunes?

A compelling example of the effort put forward in this book is the story of the anthrax attacks of September 2011, penned by contributors Jessica Stern and Ronald Schouten. The authors summarize the investigation by law enforcement, extensively portray the insider, explain how the red flags the insider exhibited were ignored, and describe the institutional security and law enforcement changes that resulted from the success of the attacks. This is one of the best known and effective insider attacks, and so it is worthy not only of inclusion in the book but of some discussion here.

The investigation began shortly after the September 11, 2001 terrorist attacks in New York City and Washington, D.C. The FBI eventually focused on microbiologist Dr. Bruce Ivins of the U.S. Army Medical Research Institute of Infectious Disease (USAMRIID). Ivins' success — temporarily abetted by the FBI's initial focus on another researcher, Steven Hatfill — was due to a swirl of regulatory changes, business culture, inattention to the dangerous

signals he sent, and luck. Perhaps most disturbing, but most relevant to the mission of the book, were two key issues: the rather obvious signals he sent regarding his mental health that were not acted upon, and the circumstance of the background checks that initiated his security clearance and maintained it through several reinvestigations over 28 years.

Ivins, a product of a traumatic childhood, had been under psychiatric care since 1978. In previous years, he had committed burglaries of sorority houses in retaliation for being shunned by sorority sisters in his higher education days. Even at this early stage, his doctor knew of these acts and his more heinous desires to poison a former sorority sister he had become obsessed with. Little or nothing of this early history of aberrant behavior — which, it must be reiterated, included criminal behavior — was made part of his later security assessments. In 1980, his 20-year career with USAMRIID commenced, along with his remarkable story of mental health decline that never was red-flagged by his superiors or the security establishment, despite Ivins' revelations to those around him of his concern for his own mental health.

Ivins had obsessive relationships with female technicians who worked for him, confiding in them about his mental state. Despite some pretty strong and frightening admissions in written emails to these colleagues (he mentioned excessive drinking and a growing paranoia), the concerns were never transmitted to Ivins' superiors. When he hacked into the technicians' emails to determine what they thought of him and found some unflattering messages, he felt so betrayed that he planned to poison of one of them. Running counter-current with this aberrant behavior was his devotion to community service. Ivins was, for example, very active in his church.

His awareness of his mental troubles caused him to seek therapy. Although he had not sought help since 1980, he resumed it after a 20-year hiatus in January 2000. A major factor in his ability to pull off the anthrax attacks was the failure of his doctors to recognize his past history and the depth of his illness and to communicate their concerns to USAMRIID.

Such fragmented and failed communications had a singular effect: they failed to ban Ivins from access to biological select agents and toxins (BSATs) and the biocontainment labs where they were manipulated. (Ivins logged his time in the labs — even his unusual nighttime and weekend hours — but they were not reviewed in timely fashion). Once the FBI investigation began, Ivins did all he could to subvert it. He failed to supply untainted anthrax samples from the lab, and he tried to direct suspicion away from himself to other researchers.

The red flags that permeate Ivins' duplicitous and secretive behavior were missed. This was due to the normalization of his behavior. In short, his colleagues became used to "Ivins being Ivins." He became the harmless eccentric.

USAMRIID investigators never spoke to the clinicians and therapists who treated Ivins. Some of these mental health specialists were extremely concerned about Ivins, diagnosing him as a sociopath and homicidal. Over the years, Ivins did complete mental health and security review forms. Although inconsistent in his entries, the information he did supply was telling but was never followed up on. No one save his private clinicians knew of his mental condition, and they were unaware of his work with BSAT. The crucial connection to dangerous materials was never made. Some of these clinicians later indicated that they would have recommended restricting him from BSATs. Although the background check system (largely forms to fill out) was deemed a sufficient practice to approve clearance to work at USAMRIID, it failed to capture Ivins' use of antipsychotic medicine.

Organizational bias also was a factor. In addition to Ivins being a familiar face with known eccentricities, leadership was apparently unwilling to change security measures without a proven outcome — that is, the removal of an insider threat. This attitude is an example of "Not in My Organization," the bias that an insider threat simply could not exist at one's place of employment. The end result of all this: Ivins was able to mail anthrax spores to offices of the *New York Times*, the *New York Post*, and the *National Enquirer*. Senate Majority Leader Tom Daschle and Senator Patrick Leahy also received letters. By November 2001, five people were dead and 17 infected. Investigators took nearly 7 years to zero in on Ivins, who became increasingly distressed by the pressure put on him by law enforcement. He committed suicide in July 2008.

As indicated by this summary, contributors Stern and Schouten provide all the necessary background material for the reader to make sense of the insider threat, including the perpetrator's motives and the security failures that enabled the threat to succeed. An equally detailed analysis of these failures and the steps taken to overcome the deficiencies are part of the book's objectives and appear to be sound advice, even if the reader does not immediately see the connection to nuclear facility operations. It does become quite clear later that this is a book about organizational failure to which nuclear facilities of all types are vulnerable.

Other insider threat events that are analyzed in the book include the Fort Hood, Texas, Terrorist Attack of 2009, in which U.S. Army Major Nidal Hasan killed 13 Defense Department employees (by Amy B. Zegart). Another chapter covers the multiple Afghan National Security Force attacks on the International Security Assistance Force from 2001 to roughly 2014 (Austin Long). Another seeks to summarize the lessons learned from the security programs in the pharmaceutical and casino industries (Bunn and Kathryn M. Glynn). A final chapter presents a worst practices guide gleaned from these insider threat reviews (Bunn and Sagan again). Here, they analyze 10 assumptions made by management and security forces that can lead to insider threat success. For example, the reader will find sections on "Assume That Serious Insider Problems Exist Elsewhere Are Not in My Organization (NIMO)," "Assume that Background Checks Will Catch All Insider Threats," and "Assume that Organizational Culture and Employee Disgruntlement Don't Matter." They are not ranked in importance or frequency of occurrence. All matter and apparently contribute equally to the problem.

A book that goes into this much detail about non-nuclear issues had better be a good read for those in nuclear non-proliferation, or else it is likely to be ignored. *Insider Threats* does not disappoint. Aside from the intriguing recounts of the incidents, the writing is clear, concise, and consistently interesting. The few black-and-white illustrations, tables, and figures are concise and useful. The book is supported by a serviceable index of about six pages.

This is a thought-provoking book that goes outside our customary playing field of nuclear non-proliferation. Focused on security and, at that, a narrower problem within the security universe, this book brings a new perspective to the issue of insider threats by utilizing the larger world's experience with this ever-present danger. It is a good example of reaching out beyond traditional boundaries for the purposes of seeking new insights. As such, it quietly achieves its scholarly mission.