A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes

Matthew Bunn and Scott D. Sagan

AMERICAN ACADEMY OF ARTS & SCIENCES

A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes

Matthew Bunn and Scott D. Sagan

This publication is available online at http://www.amacad.org/gnf.

Suggested citation: 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).

Cover image: A man walks inside a newly opened dry spent fuel storage facility. © Reuters/Stoyan Nenov.

ISBN: 0-87724-097-3

Please direct inquiries to:
American Academy of Arts and Sciences
136 Irving Street
Cambridge, MA 02138-1996
Telephone: 617-576-5000
Fax: 617-576-5050
Email: aaas@amacad.org
Web: www.amacad.org

Contents

Acknowledgments

The authors would like to thank all of the participants in the December 2011 American Academy of Arts and Sciences workshop on Insider Threats held at the Center for International Security and Cooperation (CISAC) at Stanford University. In addition, we thank Roger Howsley, Executive Director of the World Institute of Nuclear Security (WINS), for inviting us to present some of our preliminary findings on this subject at WINS workshops in Vienna, Austria, and in Johannesburg, South Africa. We also express our gratitude to the participants in the CISAC Nuclear Studies Reading Group, sponsored by the John D. and Catherine T. MacArthur Foundation, at which a first draft of this paper was presented, and to the International Atomic Energy Agency for hosting the conference on International Nuclear Security in July 2013, where some of these ideas were also presented.

Matthew Bunn thanks Nickolas Roth and Laura Dismore and Scott Sagan thanks Anna Coll and Reid Pauly for their research assistance related to this paper. Both of us also thank Francesca Giovannini for her superb work as the program officer for the Global Nuclear Future Initiative at the American Academy. Our collaborative work has been made immeasurably better by the dedicated support from and careful research conducted by these talented members of the next generation of international security specialists.

Finally, on behalf of the American Academy of Arts and Sciences, we would like to thank the foundations that have allowed us to work on Insider Threats and on other nuclear related issues throughout the course of the Academy's Global Nuclear Future Initiative. We are deeply grateful to Carnegie Corporation of New York, The William and Flora Hewlett Foundation, The John D. and Catherine T. MacArthur Foundation, The Alfred P. Sloan Foundation, the Flora Family Foundation, and the Kavli Foundation for their support.

A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes

Matthew Bunn and Scott D. Sagan

Insider threats are perhaps the most serious challenges that nuclear security systems face.[1] All of the cases of theft of nuclear materials where the circumstances of the theft are known were perpetrated either by insiders or with the help of insiders; given that the other cases involve bulk material stolen covertly without anyone being aware the material was missing, there is every reason to believe that they were perpetrated by insiders as well. Similarly, disgruntled workers from inside nuclear facilities have perpetrated many of the known incidents of nuclear sabotage. The most recent example of which we are aware is the apparent insider sabotage of a diesel generator at the San Onofre nuclear plant in the United States in 2012; the most spectacular was an incident three decades ago in which an insider placed explosives directly on the steel pressure vessel head of a nuclear reactor and then detonated them.[2] While many such incidents, including the two just mentioned, appear to have been intended to send a message to management, not to spread radioactivity, they highlight the immense dangers that could arise from insiders with more malevolent intent. As

1. This paper draws on an earlier paper by Scott D. Sagan, "Insider Threats in Comparative Perspective," IAEA-CN-203-156, in *Proceedings of International Nuclear Security: Enhancing Global Efforts*, Vienna, July 1–5, 2013 (Vienna: International Atomic Energy Agency, 2013).

2. For more on the San Onofre incident, see Jeff Beattie, "Sabotage Eyed in Generator Incident at San Onofre Nuke," *Energy Daily*, December 3, 2012. Engine coolant was found in the oil system of one of the plant's diesel generators—a crucial safety system in the event of loss of offsite power—which would have caused the generator to fail if needed. The plant was shut down at the time. An internal investigation found "evidence of potential tampering as the cause of the abnormal condition," as the company reported to the Nuclear Regulatory Commission (NRC). The explosive attack on the pressure vessel occurred at the Koeberg nuclear power plant in South Africa in 1982, before the plant had begun operating. It was perpetrated by a white South African fencing champion, Rodney Wilkinson, in league with the African National Congress. See, for example, David Beresford, "How We Blew Up Koeberg (. . . and Escaped on a Bicycle)," *Mail & Guardian* (South Africa), December 15, 1995. Beresford has offered a more detailed account, based on interviews with the perpetrator, in *Truth is a Strange Fruit: A Personal Journey Through the Apartheid War* (Auckland Park, South Africa: Jacana Media, 2010), 102–107. We are grateful to Tom Bielefeld for providing this reference. These are but two of a stream of cases that has continued for decades. Three decades ago, an NRC study identified "32 possibly deliberate damaging acts at 24 operating reactors and reactor construction sites" from 1974 to 1980—most of them attributed to insiders. See Matthew Wald, "Nuclear Unit Gets Sabotage Warning," *The New York Times*, June 8, 1983.

it turns out, insiders perpetrate a large fraction of thefts from heavily guarded non-nuclear facilities as well.[3] Yet organizations often find it difficult to understand and protect against insider threats. Why is this the case?

Part of the answer is that there are deep organizational and cognitive biases that lead managers to downplay the threats insiders pose to their nuclear facilities and operations. But another part of the answer is that those managing nuclear security often have limited information about incidents that have happened in other countries or in other industries, and the lessons that might be learned from them.

In the world of nuclear *safety*, sharing of incidents and lessons learned is routine, and there are regularized processes for it, through organizations such as the International Atomic Energy Agency (IAEA) and the World Association of Nuclear Operators (WANO). Nothing comparable exists in nuclear security.[4]

Otto von Bismarck once said that only a fool learns from his mistakes; a wise man learns from the mistakes of others. This paper is intended to help nuclear security operators learn from the mistakes of others in protecting against insider threats, drawing on episodes involving intelligence agencies, the professional military, bodyguards for political leaders, banking and finance, the gambling industry, and pharmaceutical manufacturing. It is based in part on a 2011 workshop hosted by the American Academy of Arts and Sciences at the Center for International Security and Cooperation at Stanford University that brought together experts to compare challenges and best practices regarding insider threats across organizations and industries.

The IAEA and the World Institute for Nuclear Security (WINS) produce "best practices" guides as a way of disseminating ideas and procedures that have been identified as leading to improved security. Both have produced guides on protecting against insider threats.[5] But sometimes mistakes are even more instructive than successes.

Here, we are presenting a kind of "worst practices" guide of serious mistakes made in the past regarding insider threats. While each situation is unique, and serious insider problems are relatively rare, the incidents we describe reflect issues that exist in many contexts and that every nuclear security manager should consider. Common organizational practices—such as prioritizing production over security, failure to share information across subunits, inadequate rules or inappropriate waiving of rules, exaggerated faith in group loyalty, and excessive

3. Bruce Hoffman, Christina Meyer, Benjamin Schwarz, and Jennifer Duncan, *Insider Crime: The Threat to Nuclear Facilities and Programs* (Santa Monica, Calif.: RAND, 1990).

4. Matthew Bunn, "Strengthening Global Approaches to Nuclear Security," IAEA-CN-203-298, in *Proceedings of International Nuclear Security: Enhancing Global Efforts*, Vienna, July 1–5, 2013 (Vienna: International Atomic Energy Agency, 2013).

5. International Atomic Energy Agency, *Preventive and Protective Measures Against Insider Threats*, Security Series No. 8 (Vienna: IAEA, 2008); and World Institute for Nuclear Security, *Managing Internal Threats: A WINS International Best Practice Guide for Your Organization* (Vienna: WINS, 2010).

focus on external threats—can be seen in many past failures to protect against insider threats.

LESSONS

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

Some organizations, like companies in the diamond-mining industry or the gambling industry, assume that their employees may be thieves. They accept that relatively low-consequence insider theft happens all the time, despite employee screening and inspections designed to prevent it.

By contrast, organizations that consider their staff to be part of a carefully screened elite—including intelligence agencies and many nuclear organizations, among others—often have strong internal reasons to stress and reinforce the loyalty and morale of their employees in order to encourage more effective operations. They also sometimes have incentives to encourage perceptions that competitors do not have the same levels of loyalty. The repeated stress on the high loyalty of one's organization when compared to others can lead management to falsely assume that insider threats may exist in other institutions, but not in their organization.

A dramatic case in point was the failure to remove Sikh bodyguards from Indian Prime Minister Indira Gandhi's personal security unit after she had instigated a violent political crackdown on Sikh separatists in 1984. In June 1984, Operation Blue Star targeted Sikh separatists who had taken over the Golden Temple in Amritsar.[6] Extra security personnel were deployed at the prime minister's residence after a series of death threats were made against the prime minister and her family. According to H. D. Pillai, the officer in charge of Gandhi's personal security, "[T]he thrust of the reorganized security . . . was to prevent an attack from the outside. . . . What we did not perceive was that an attempt would be made inside the Prime Minister's house."[7] When it was suggested by other officials that Sikh bodyguards should be placed only on the outside perimeter of the prime minister's compound, Mrs. Gandhi insisted that this could not be done without damaging her political reputation: "How can I claim to be secular if people from one community have been removed from within my own house?"[8] On October 31, 1984, two Sikh guards—one a long-standing bodyguard (Beant Singh, the personal favorite of Mrs. Gandhi) and the other a newly added guard (Satwant Singh)—conspired and assassinated Mrs. Gandhi.

6. For more detail, see Scott D. Sagan, "The Problem of Redundancy Problem: Why More Nuclear Security Forces May Produce Less Security," *Risk Analysis* 24 (4) (2004): 935–946.

7. Ritu Sarin, *The Assassination of Indira Gandhi* (New Delhi: Penguin, 1990), 19.

8. Ibid.

The Gandhi case, unfortunately, was not unique. While Pervez Musharraf was president of Pakistan, he survived at least two near-miss assassination attempts, both of which were perpetrated by active Pakistani military personnel in league with al-Qaeda.[9] Similarly, Ahmed Wali Karzai, a powerful Afghan regional official and the brother of the Afghan president, was assassinated in 2011 by his principal security guard, a trusted confidant who had worked with the family for seven years.[10]

These cases offer several key lessons. First, and most fundamentally, organizational leaders should never assume that their personnel are so loyal that they will never be subject to ideologies, shifting allegiances, or personal incentives that could lead them to become insider threats. Managers should beware of the "halo effect," in which well-liked employees are assumed to be trustworthy (a special case of *affect bias*, the tendency we all have to assume that something we like for a particular reason has other positive qualities as well).[11]

Second, managers should understand that guards themselves can be part of the insider threat—"the most dangerous internal adversaries," in the words of a senior Russian nuclear security manager.[12] Indeed, according to one database, guards were responsible for 41 percent of insider thefts at non-nuclear guarded facilities.[13] Hence, managers should not assume that adding more guards automatically leads to increased security.[14] Finally, individual leaders or facility managers should not countermand security professionals' judgments solely for personal or political reasons.

Lesson #2: Don't Assume that Background Checks will Solve the Insider Problem

The belief that personnel who have been through a background check will not pose an insider problem is remarkably widespread—a special case of the "not in my organization" fallacy. There are two reasons why this belief is mistaken. First, background checks are often not very effective. Second, even completely trustworthy employees may become insiders, especially if they are coerced.

9. See, for example, "Escaped Musharraf Plotter Was Pakistan Air Force Man," *Agence France Presse*, January 12, 2005; and "Musharraf Al-Qaeda Revelation Underlines Vulnerability: Analysts," *Agence France Presse*, May 31, 2004.

10. Bashir Ahmad Naadem, "Suspects Arrested in Wali Assassination," *Pajhwok Afghan News*, July 12, 2011.

11. For the halo effect, see Richard E. Nisbett and Timothy D. Wilson, "The Halo Effect: Evidence for Unconscious Alteration of Judgments," *Journal of Personality and Social Psychology* 35 (4) (April 1977): 250–256. For a discussion of affect bias (and other biases likely to be important to nuclear security managers), see Daniel Kahneman, Paul Slovic, and Amos Tversky, eds., *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge: Cambridge University Press, 1982).

12. Igor Goloskokov, "Refomirovanie Voisk MVD Po Okhrane Yadernikh Obektov Rossii [Reforming MVD Troops to Guard Russian Nuclear Facilities]," trans. Foreign Broadcast Information Service, *Yaderny Kontrol* 9 (4) (Winter 2003).

13. Hoffman et al., *Insider Crime*.

14. Sagan, "The Problem of Redundancy Problem."

Background checks as they are conducted today often fail to catch indicators of potential problems. Even in-depth, ongoing monitoring can miss key insider issues: after all, Aldrich Ames famously passed lie detector tests. Moreover, in many cases at non-nuclear facilities, there was no indication that employees were not trustworthy until long after they were hired: they became criminals only once on the job. This was the case with the trusted guards discussed in the previous section; and Leonid Smirnov, who perpetrated one of the first well-documented thefts of weapons-usable nuclear material (1.5 kilograms of 90 percent enriched HEU from the Luch Production Association in Podolsk in 1992), was a trusted employee who had worked at the facility for many years.[15]

Even if all the insiders at a facility are highly reliable, coercion remains a danger. In a case in Northern Ireland in 2004, for example, thieves allegedly linked to the Provisional Irish Republican Army made off with £26 million from the Northern Bank. The bank's security system was designed so that the vault could be opened only if two managers worked together, but the thieves kidnapped the families of two bank managers and blackmailed them into helping the thieves carry out the crime.[16] (The thieves also used deception in this case, appearing at the managers' homes dressed as policemen.) No background check or ongoing employee monitoring system can prevent insiders from acting to protect their families. Terrorists (as the Northern Bank thieves may have been) also make use of such coercion tactics, and might do so to enlist help in a theft of nuclear material, rather than money. For example, kidnapping in order to blackmail family members into carrying out certain actions has been a common Chechen terrorist tactic.[17] An examination of a range of major crimes concluded that such coercion tactics are frequently successful.[18]

The lesson here is clear: while it is important to have programs that screen employees for trustworthiness and monitor their behavior once employed, no one should ever assume that these programs will be 100 percent effective. Measures to prevent insider theft are needed even when a manager believes all of his employees are likely to be completely trustworthy.

15. For interviews with Smirnov, see *Frontline*, "Loose Nukes: Interviews" (Public Broadcasting System, original air date November 19, 1996), http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/; and Ginny Durrin and Rick King, *Avoiding Armageddon*, episode 2, "Nuclear Nightmares: Losing Control" (Ted Turner Documentaries, 2003), http://www.pbs.org/avoidingarmageddon.

16. For a good introduction to the Northern Bank case, see Chris Moore, "Anatomy of a £26.5 Million Heist," *Sunday Life*, May 21, 2006. One of the managers, Chris Ward, was subsequently charged with being a willing participant in the crime, and the kidnapping of his family a sham. Ward denied the charges and was subsequently acquitted. See Henry McDonald, "Employee Cleared of £26.5 Million Northern Bank Robbery," *Guardian*, October 9, 2008.

17. Robyn Dixon, "Chechnya's Grimmest Industry: Thousands of People Have Been Abducted by the War-Torn Republic's Kidnapping Machine," *Los Angeles Times*, September 18, 2000.

18. Robert Reinstedt and Judith Westbury, *Major Crimes as Analogs to Potential Threats to Nuclear Facilities and Programs*, N-1498-SL (Santa Monica, Calif.: RAND, 1980).

Lesson #3: Don't Assume that Red Flags will be Read Properly

High-security facilities typically have programs to monitor the behavior of employees for changes that might suggest a security issue, and to encourage other employees to report such changes. Effective personnel screening, training, and monitoring systems are designed to pick up subtle signs that personnel reliability has been or is about to be compromised by disgruntlement, mental health problems, drug abuse, or personal life difficulties, or that security reliability has been or is about to be compromised by shifting political allegiances, corruption, recruitment, or self-radicalization. While picking up subtle signs of danger is difficult, security managers often assume that severe red flags warning of problems will not go unnoticed. But if individual incentive systems and information-sharing procedures encourage people not to report, even the reddest of red flags can be ignored.

The shooting incident at Fort Hood, Texas, is an extreme version of this problem. On November 5, 2009, U.S. Army Major Nidal Hasan opened fire on a group of soldiers preparing to deploy to Afghanistan, killing thirteen and wounding twenty-nine.[19] Major Hasan had made no secret of his radicalized, violent beliefs, voicing his justification of suicide bombers, defense of Osama bin Laden, and devotion to Sharia law over the U.S. Constitution to peers and supervisors over a period of *years* before the attack. The San Diego Joint Terrorism Task Force (JTTF), an interagency group managed by the FBI, had also obtained multiple email communications between Hasan and a "foreign terrorist" reported in the press to be Anwar al-Awlaki.[20] As Amy Zegart has argued, stopping "a radicalized American Army officer who was publicly espousing his beliefs and was known to be communicating with one of the world's most dangerous and inspirational terrorists in the post-9/11 era was not asking the impossible."[21]

Why did multiple U.S. government processes fail to act on the obvious red flags raised by Hasan? There were several reasons. First, the process for review and removal of an officer on security reliability grounds was time-consuming and cumbersome, posing an immense set of headaches to anyone who tried to act. Combined with the incentive to keep someone with Hasan's psychiatry specialty in the service, no officer at Walter Reed decided to start proceedings against Hasan. Second, the Army's system for reviewing officers' performance

19. This case study is based on Amy Zegart, "The Fort Hood Terrorist Attack: An Organizational Postmortem on DOD and FBI Deficiencies," working paper, March 20, 2013.

20. U.S. Committee on Homeland Security and Governmental Affairs, *A Ticking Time Bomb: Counterterrorism Lessons from the U.S. Government's Failure to Prevent the Fort Hood Attack*, Special Committee Report [hereafter Senate Report], 112th Cong., 1st sess., February 3, 2011, pp. 28–31; Sebastian Rotella and Josh Meyer, "Fort Hood's Suspect Contact with Cleric Spelled Trouble, Experts Say," *Los Angeles Times*, November 12, 2009; Carrie Johnson, "FBI to Probe Panels that Reviewed Emails from Alleged Fort Hood Gunman," *The Washington Post*, December 9, 2009; and Carrie Johnson, Spencer S. Hsu, and Ellen Nakashima, "Hasan had Intensified Contact with Cleric," *The Washington Post*, November 21, 2009.

21. Zegart, "The Fort Hood Terrorist Attack."

failed to compile the relevant information in a usable way. There were two sets of files for each officer. Personal files were quite detailed, but kept only at the local level and destroyed when a service member moved on, making it impossible to track behavior from one assignment to the next. Officer Evaluation Reports (OERs) had only yes/no judgments on standardized questions, combined with an overall rating of an officer's suitability for promotion; given the shortage of middle-grade officers in the post–Cold War military, there were substantial pressures not to make trouble by giving poor ratings, and every OER that Hasan received was positive, despite his alarming statements and abysmally poor performance in his job. As a Senate investigation found, Hasan's reviews "flatly misstated" his actual performance and made no mention of the red flags he was repeatedly raising.[22] Third, as often happens in organizational settings, significant social shirking occurred, as there was ample opportunity to pass difficult responsibilities on to someone else. Hasan was moving soon from Walter Reed to Fort Hood, and officers at the former base knew that as long as they did nothing to raise any issues about his transfer, they would not have to deal with him anymore. (The wonderful phrase used to describe the practice of writing positive reviews of poor-performing service members so that they can be shipped to another command is "packaged for export.") Fourth, at least some officers feared that actions taken to discipline a Muslim officer for his political statements would have been perceived as discriminatory.

Fifth, there was a severe lack of information sharing between Army security specialists and the JTTF, which had responsibility for evaluating the intercepted email messages between Hasan and al-Awlaki, and between different JTTF offices. The San Diego JTTF wanted an investigation of the email communication that it had found, but the Washington office had jurisdiction and did not give Hasan as high a priority as the San Diego office thought justified. Due to problems with their information systems and misunderstandings between them, both the San Diego JTTF and the Washington JTTF thought the other was monitoring Hasan's continued communications, when in fact neither was. In the end, the only investigation that the Washington JTTF performed was a review of Hasan's OERs, which found only positive reports—and "some even sanitized his obsession with Islamic extremism as praiseworthy research."[23] No one looked at Hasan's local records, interviewed him, or spoke to any of his colleagues or superiors. Hence, a junior Department of Defense official in the Washington JTTF, after reviewing the positive OERs, made the tragic and controversial decision that Hasan's email conversations with al-Awlaki were just part of a research project; he therefore did not feel the need to pass on the intelligence reports to Hasan's superior officers.

The lessons here are disturbing. When individual and group incentives push against objective analysis of warning signals, and when, as often happens

22. Discussed in ibid.

23. Ibid.

in compartmentalized security organizations, information sharing is restricted, even the reddest of red flags can be ignored.

Nuclear managers may assume that their systems for detecting red flags are much better—that they would surely catch someone like Hasan. But the case of Sharif Mobley suggests that this may not always be the case. In March 2010, Mobley was arrested in Yemen for alleged involvement in al-Qaeda and for shooting a guard in an attempt to escape. Yet between 2002 and 2008, prior to traveling to Yemen, Mobley worked at five U.S. nuclear power plants (Salem-Hope Creek, Peach Bottom, Limerick, Calvert Cliffs, and Three Mile Island), where he was given unescorted access inside the plant (though not in the vital areas) to perform maintenance and carry supplies. According to a Nuclear Regulatory Commission (NRC) report, Mobley voiced his militant views during his work, referring to non-Muslim coworkers as "infidels" and remarking to some in his labor union: "We are brothers in the union, but if a holy war comes, look out."[24] Though the rules in place at the time required individual workers to report any suspicious behavior on the part of coworkers, none of Mobley's fellow union members apparently reported these statements. The red flags were again invisible.

Cases of ignoring red flags as extreme as Hasan's, or even Mobley's, do not happen often. But the issues raised—failing to report problems because of the headaches involved, passing troublesome employees off to someone else—arise in smaller ways in almost every organization. Indeed, research suggests that indicators of insider security problems are systematically underreported.[25] One study of several cases of insider information-technology sabotage in critical infrastructure found that 97 percent of the insiders involved in the cases "came to the attention of supervisors or coworkers for concerning behavior prior to the attack," but the observed behavioral precursors were "ignored by the organization."[26]

All managers of nuclear organizations should be asking themselves: how are the incentives for reporting such issues *really* aligned in my organization? How could I test how well such issues are reported? How could I improve my organization's ability to detect and act on a potential problem before it occurs?

24. Scott Shane, "Worker Spoke of Jihad, Agency Says," *The New York Times*, October 4, 2010, http://www.nytimes.com/2010/10/05/us/05mobley.html?_r=0 (accessed May 19, 2013); and Peter Finn, "The Post-9/11 Life of an American Charged with Murder," *The Washington Post*, September 4, 2010, http://www.washingtonpost.com/wp-dyn/content/article/2010/09/04/AR2010090403334.html (accessed May 19, 2013).

25. Suzanne Wood and Joanne C. Marshall-Mies, *Improving Supervisor and Co-Worker Reporting of Information of Security Concern* (Monterey, Calif.: Defense Personnel Security Research Center, January 2003). Subsequently, researchers from the same center developed an improved reporting system now used in the Department of Defense, and the reporting system may be of interest to nuclear security managers. See Suzanne Wood, Kent S. Crawford, and Eric L. Lang, *Reporting of Counterintelligence and Security Indicators by Supervisors and Coworkers* (Monterey, Calif.: Defense Personnel Security Research Center, May 2005).

26. Andrew P. Moore, Dawn M. Capelli, and Randall F. Trzeciak, *The "Big Picture" of Insider IT Sabotage Across U.S. Critical Infrastructures*, CMU/SEI-2008-TR-2009 (Pittsburgh: Software Engineering Institute, Carnegie Mellon University, May 2008).

Lesson #4: Don't Assume that Insider Conspiracies are Impossible

Conspiracies of multiple insiders, familiar with the weaknesses of the security system (and in some cases including guards or managers), are among the most difficult threats for security systems to defeat. Many nuclear security systems include only a single insider in the threats they are designed to protect against. And many nuclear security experts do not see groups of insiders as a credible threat: in a recent survey of nuclear security experts from most of the countries where HEU and separated plutonium exist, most agreed that a single insider was a highly credible threat; but no one rated multiple insiders as highly credible, and only a few rated insider conspiracies as "somewhat credible."[27]

Yet insider conspiracies routinely occur. In one database, they constituted approximately 10 percent of the crimes examined.[28] In 1998, for example, an insider conspiracy at one of Russia's largest nuclear weapons facilities attempted to steal 18.5 kilograms of HEU—potentially enough for a bomb.[29] The Northern Bank case described above is another example, involving two trusted, senior insiders working together—both under coercion from threats to their families. The Gandhi case is yet another example—again involving two insiders working together, both trusted enough to be personal guards to the prime minister. The fact that two of the major cases selected above to illustrate other points also involved insider conspiracies is a telling indicator of how important such conspiracies are.

The lesson here is clear: wherever possible, nuclear security systems should be designed to offer substantial protection against even a small group of insiders working together. Nuclear security managers should set up "red team" processes for identifying approaches that groups of insiders might use to steal material and for finding cost-effective approaches to stop them.

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

Many managers have high confidence in particular elements of their security system, from a particularly well-trained guard force to portal monitors at every exit. Many such systems, however, are much more vulnerable to being defeated

27. Matthew Bunn and Eben Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World: Results of a Survey* (Cambridge, Mass.: Project on Managing the Atom, Harvard Kennedy School, March 2014), http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf.

28. Hoffman et al., *Insider Crime*.

29. This attempt was first revealed by the Russian Federal Security Service (FSB), which claimed credit for foiling it. See Yevgeniy Tkachenko, "FSB Agents Prevent Theft of Nuclear Materials," *ITAR-TASS*, December 18, 1998. The attempt was discussed in somewhat more detail by Victor Erastov, chief of material accounting for what was then Russia's Ministry of Atomic Energy; see "Interview: Victor Yerastov: MINATOM Has All Conditions for Providing Safety and Security of Nuclear Material," *Yaderny Kontrol Digest* 5 (1) (Winter 2000). Neither of those accounts identified the type of material; that is from a 2000 interview by Matthew Bunn with a Ministry of Atomic Energy official.

than they first appear—especially to insiders, who may be among the staff who know how they work.

Portal monitors are one example; they are essential but imperfect. In discussion with Matthew Bunn, a Livermore security expert described a meeting with representatives of a portal-monitor production firm who had very high confidence in their product's ability to detect nuclear material. The company gave the security expert a radioactive test sample that they were confident their system could detect, and in three times out of five, he was able to carry it through the monitor without detection.

Or consider the case of tamper-indicating devices (TIDs), also known as seals, widely used to indicate whether any material has been removed or tampered with. Many people believe that an unbroken seal shows with high confidence that the sealed item has not been disturbed. Yet a study of 120 types of seals in common commercial and government use found that all 120 could be defeated in ways that would not be detected by the seal inspection protocols in use. Tampering was possible with materials available from any hardware store, and with defeat times averaging about five minutes.[30] The TIDs included sophisticated fiber-optic seals, among others; some of these high-tech options did not perform as well, when used as people in the field actually use them, as lower-tech methods.

In short, security managers should never have too much faith in any one element of their security system. Seals can be defeated, portal monitors can be defeated or gone around, guards can fail to search employees, employee reporting systems can fail to detect suspicious behavior. But with a system that genuinely offers defense in depth, it can be made very difficult for an insider adversary to overcome all the layers in the system.

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

Nuclear organizations often have an engineering culture, focused more on the technology than on the people using it. Managers sometimes assume that as long as the right systems and procedures are in place, employees will follow the procedures and everything will be fine. In most countries, including the United States, regulators do not require operators to take any steps to ensure a strong security culture, or even to have a program to assess and improve security culture that regulators can review.

But the reality is that the culture of an organization and the attitudes of the employees have a major impact on security. As General Eugene Habiger, former Department of Energy "security czar" and former commander of U.S. strategic forces, put it, "Good security is 20 percent equipment and 80 percent culture."[31]

30. Roger G. Johnston, "Tamper-Indicating Seals for Nuclear Disarmament and Hazardous Waste Management," *Science & Global Security* 9 (2001): 93–112.

31. From an April 2003 interview by Matthew Bunn.

A visit by Matthew Bunn to a Russian nuclear institute in the mid-2000s provides an example of the impact of security culture on insider protection. In the hallway leading to the vault where a substantial amount of weapons-grade nuclear material was stored, there were two portal monitors that personnel had to pass through, one after the other, an American machine and a Russian machine. When asked why, the site official conducting the tour said that the building next door made medical isotopes, and on Thursdays, when the chemical separations were done to get the desired isotopes from the remainder, so much radiation went up the stack that it set off the American-made portal monitor. So on Thursdays, they turned off the American-made monitor and relied on the less sensitive Russian one. Of course, every insider was aware of this practice, and would know to plan an attempted theft for a Thursday, making the existence of the American portal monitor largely pointless.

A photograph from a 2001 U.S. General Accounting Office report provides a similar example: it shows a wide-open security door at a Russian facility. What is remarkable is that the door was propped open on the very day the American auditors were there to photograph it being propped open, suggesting that the staff did not see this as a problem.[32]

Perhaps the most spectacular recent incident caused by a breakdown of security culture was the intrusion by an 82-year-old nun and two other protesters at the Y-12 facility in Tennessee in 2012. The protesters went through four layers of fences, setting off multiple intrusion detectors, but no one bothered to check the alarms until the protesters had spent some time hammering and pouring blood directly on the wall of a building where enough weapons-grade HEU metal for thousands of nuclear weapons is stored. As it turns out, a new intrusion detection system had been setting off ten times as many false alarms as the previous system had, yet this was tolerated; cameras to allow guards to assess the cause of the alarms had been broken for months, and this was also tolerated. The guards apparently had gotten sick of checking out all the alarms, and even the heavily armed guards inside the building did not bother to check when they heard the hammering, assuming that it must have been construction work they had not been told about (even though this all took place before dawn).[33]

To avoid such problems, nuclear managers should seek to build a culture in which all employees take security seriously and count it as an important part of their mission—all day, every day. They must also foster employees' understanding that security is everyone's responsibility, not something only the security

32. U.S. Congress, General Accounting Office, *Security of Russia's Nuclear Material Improving, More Enhancements Needed*, GAO-01-312 (Washington, D.C.: GAO, February 2001).

33. See, for example, C. Donald Alston, Letter to Secretary of Energy Steven Chu, December 10, 2012, http://pogoarchives.org/m/nss/20121210-alston-ltr.pdf; Norman Augustine, Letter to Secretary of Energy Steven Chu, December 6, 2012, http://pogoarchives.org/m/nss/20121210-augustine-ltr.pdf; Richard Meserve, Letter to Secretary of Energy Steven Chu, December 6, 2012, http://pogoarchives.org/m/nss/20121206-meserve-ltr.pdf; and Office of the Inspector General, U.S. Department of Energy, *Inquiry Into the Security Breach at the National Nuclear Security Administration's Y-12 National Security Complex*, DOE/IG-0868 (Washington, D.C.: DOE, August 2012), http://energy.gov/sites/prod/files/IG-0868_0.pdf.

team has to worry about.[34] Establishing clear incentives that make employees understand that they will be rewarded for good security performance is one key element of building such a culture, and of making clear the priority that management places on security.[35]

Employee satisfaction is another critical aspect of organizational culture. Disgruntled employees are much more likely to become insiders—and much less likely to proactively help to improve security by reporting odd or suspicious behavior or by creatively looking for security vulnerabilities and ways to fix them. In situations ranging from retail theft to IT sabotage, disgruntlement has been found to be a key driver of insider threats.

In the study of IT sabotage cases mentioned above, the authors found that 92 percent of the cases examined occurred "following a negative work-related event such as termination, dispute with a current or former employer, demotion, or transfer." Well over half of the insiders in these cases were already perceived in the organization to be disgruntled.[36]

Fortunately, organizations have found that it is not very difficult or expensive to combat employee disgruntlement. Providing complaint and ombudsman processes that are perceived to result in actions to address the issues; complimenting and rewarding employees for good work; addressing the problem of bullying bosses: these and other steps can go a long way toward reducing disgruntlement and its contribution to the insider threat.[37]

It is not known how much of a contribution disgruntlement makes to the probability of an insider taking more serious actions, such as stealing nuclear material or sabotaging a nuclear facility. Nevertheless, for both safety and security reasons, nuclear managers should strive to build a strong, performance-oriented culture in which employees believe that they are respected and treated well, and in which they have avenues for their complaints and ideas to be heard.

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

Many individuals involved in the nuclear security field have backgrounds in engineering and nuclear safety, where the goal is to protect against natural disasters and accidents, not against reactive adversaries. This can produce a compliance-oriented approach to security: a belief that once systems are in place

34. On the importance of this point, see World Institute for Nuclear Security, *Nuclear Security Culture: A WINS Best Practice Guide for Your Organization*, revision 1.4 (Vienna: WINS, September 2009).

35. Matthew Bunn, "Incentives for Nuclear Security," *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management,* Phoenix, Ariz., July 10–14, 2005 (Northbrook, Ill.: INMM, 2005); available at http://belfercenter.ksg.harvard.edu/files/inmm-incentives2-05.pdf.

36. Moore, Capelli, and Trzeciak, *The "Big Picture" of Insider IT Sabotage*.

37. See Roger G. Johnston, "Mitigating the Insider Threat (and Other Security Issues)," http://www.ne.anl.gov/capabilities/vat/pdfs/Insider%20Threat%20and%20Other%20Security%20Issues.pdf.

that are assessed to be capable of beating the adversaries included in the design basis threat (DBT) on the pathways designers identified, the security system will be effective. But reactive adversaries will observe the security systems and the pathways they protect against, and they will think of other pathways. Insider threats are a particularly dangerous form of reactive adversary because insiders are well placed to understand the organization's security procedures and their weaknesses.

The best case to illustrate this point is that of Robert Hanssen, the senior FBI analyst convicted in 2001 on fifteen counts of espionage, in what the FBI has called "possibly the worst intelligence disaster in U.S. history."[38] According to the 2003 Department of Justice report on the case, Hanssen's initial decision to engage in espionage "arose from a complex blend of factors, including low self-esteem and a desire to demonstrate intellectual superiority, a lack of conventional moral restraints, a feeling that he was above the law, a lifelong fascination with espionage and its trappings and a desire to become a 'player' in that world, the financial rewards he would receive, and the lack of deterrence—a conviction that he could 'get away with it.'"[39] His espionage activities often raised alarm bells, but his insider advantage let him avoid detection in three key ways. First, Hanssen was capable of being uniquely reactive to counterintelligence investigations because of his placement within the FBI counterintelligence bureaucracy. Second, Hanssen was able to alter his contact procedures with his Russian associates whenever he felt that he was close to being caught; he was even able to search for his own name within the FBI internal database to monitor whether he was the subject of any investigation.[40] Third, Hanssen knew how to avoid movement within the FBI bureaucracy that would have subjected him to polygraph examinations.[41]

In other contexts, this problem—that insiders can observe and work around security measures—comes up again and again. In a study of insider crimes that might be analogous to insider thefts or attacks at nuclear facilities, the authors repeatedly found that the success of insider crimes depended on the perpetrators' observation of security vulnerabilities.[42] The study of insider IT sabotage mentioned earlier noted that the insiders overwhelmingly took advantage of their knowledge of the IT security systems, creating access pathways for them-

38. U.S. Department of Justice, Commission for Review of FBI Security Programs, "A Review of FBI Security Programs," March 2002, http://www.fas.org/irp/agency/doj/fbi/websterreport.html (accessed May 17, 2013).

39. U.S. Department of Justice, "A Review of the FBI's Performance in Deterring, Detecting, and Investigating the Espionage Activities of Robert Philip Hanssen," August 2003, http://www.justice.gov/oig/special/0308/final.pdf (accessed May 17, 2013).

40. Ibid.

41. David Wise, *Spy: The Inside Story of How the FBI's Robert Hanssen Betrayed America* (New York: Random House, 2002), 177.

42. Hoffman et al., *Insider Crime*.

selves completely unknown to the organization—in other words, they invented ways to attack that the security planners had not known were possible.[43]

There are several lessons here. First, security managers need to find creative people with a hacker's mindset to come up with a wide range of ways that insiders might try to beat the security system—and then develop security measures that will be effective against a broad range of possibilities. A security system adequate to defend against the first few pathways thought of by an unimaginative committee is not likely to be good enough against the real threat. Such uncreative vulnerability assessments were the target for Roger Johnston and his colleagues in the Vulnerability Assessment Team at Argonne National Laboratory; in their instructive and amusing set of "Security Maxims," they offer the "Thanks for Nothin'" maxim: "Any vulnerability assessment which finds no vulnerabilities or only a few is worthless and wrong."[44] Second, those with the most detailed information about how the organization protects itself against insider threats should be subject to especially strong reviews and monitoring to ensure that the organization is appropriately "guarding the guardians."

Lesson #8: Don't Assume that Security Rules are Followed

Security-conscious organizations create rules and procedures to protect valuable assets. But such organizations also have other, often competing, goals: managers are often tempted to instruct employees to bend the security rules to increase productivity, meet a deadline, or avoid inconvenience. And every hour an employee spends following the letter of security procedures is an hour not spent on activities more likely to result in a promotion or a raise.[45] Other motivations—friendships, union solidarity, and familial ties—can also affect adherence to strict security rules.

The cases here are legion; indeed, any reader who has worked for a large organization with security rules probably has direct experience of some of those rules being violated. In many cases, the security rules are sufficiently complex and hard to understand that employees violate them inadvertently. In some cases, the deviations from the rules are more substantial. In both the United States and Russia, for example, there have been cases of nuclear security guards sleeping on the job; patrolling without any ammunition in their guns (apparently because shift managers wanted to ensure that there would be no accidental firing incidents on their watch); and turning off intrusion detection systems when they got tired of checking out false alarms (arguably even worse than simply ignoring those alarms, as appears to have occurred in the Y-12 case). In one U.S. case prior to the 9/11 attacks, an inspector found a security guard at a nuclear facility asleep on duty for more than a half-hour, but the incident was not considered a serious problem

43. Moore, Capelli, and Trzeciak, *The "Big Picture" of Insider IT Sabotage*.

44. Roger G. Johnston, "Security Maxims," Vulnerability Assessment Team, Argonne National Laboratory, September 2013, http://www.ne.anl.gov/capabilities/vat/pdfs/security_maxims.pdf.

45. Bunn, "Incentives for Nuclear Security."

because no terrorists were attacking at that moment—raising issues about the security culture of both the operator and the regulator.[46]

The U.S. Department of Energy's nuclear laboratories have been known for widespread violations of security rules since the dawn of the nuclear age; during the Manhattan Project, physicist Richard Feynman was barred from certain facilities for illicitly cracking into safes and violating other rules as pranks to reveal vulnerabilities.[47] (Feynman's tales of incompetence at the lab emphasize another important lesson: do not assume that rules will be implemented intelligently.)

Incentives often drive rule-breaking. Consider, as one example, the case of cheating on security tests at Y-12 (years before the recent intrusion). In January 2004, the U.S. Department of Energy inspector general found that for many years the Wackenhut Corporation, which provided security for the Y-12 National Security Complex in Oak Ridge, Tennessee, had been cheating on its security exercises. These exercises simulated attacks on the nuclear facility, challenging the security guards to repel a mock assault. The security tests were important to the guard force: they could affect the payment the security contractor received and possibly the bonuses that security personnel themselves received. Until 2003, the Wackenhut security force received scores of "outstanding" and a total of $2.2 million in bonuses for their performances on security exercises. It was later revealed that, up to three weeks in advance of the exercises, Wackenhut management told Y-12 security officers which buildings and targets would be attacked, the exact number of adversaries, and the location where a diversion would occur. The protective force thus had ample time to formulate special plans on how to counter the adversary, and they were able to place trucks or other obstacles at advantageous points to be used as barricades and concealment by protective force responders for shooting during the exercises. The Wackenhut management also identified the best prepared protective force personnel and substituted them for less prepared personnel, and officers who would normally relieve other protective force personnel were armed and held in "standby" to participate in an exercise, potentially adding six or seven armed responders who would not normally have been available during a shift. And several participants reported that the defenders had also disabled

46. U.S. Congress, General Accounting Office, *Nuclear Regulatory Commission: Oversight of Security at Commercial Nuclear Power Plants Needs to Be Strengthened*, GAO-03-752 (Washington, D.C.: GAO, September 2003), 12, http://www.gao.gov/new.items/d03752.pdf.

47. For Feynman's account, see Richard P. Feynman, *Surely You're Joking, Mr. Feynman! Adventures of a Curious Character* (New York: W.W. Norton, 1985), 137–155. For an account of the broader record (possibly more negative than is justified), see President's Foreign Intelligence Advisory Board, *Science at Its Best, Security at Its Worst: A Report on Security Problems at the U.S. Department of Energy* (Washington, D.C.: PFIAB, June 1999), http://www.fas.org/sgp/library/pfiab/. This report includes a remarkable listing of previous reports on security weaknesses at the Department of Energy.

the sensors in their laser-tag gear, so in the tests they were essentially invincible: the system would never score them as having been shot.[48]

The lesson here is not that security procedures and personnel-screening rules are routinely violated at nuclear power facilities. They are not. Nor is the lesson that nuclear security exercises like those at Y-12 are not important—quite the opposite.

But rules are not followed universally or strictly, especially when they are in tension with other goals, such as continuing production, meeting deadlines, and maintaining collegial relations among coworkers. And tests are likely to be reliable only when they are independent and uncompromised. Nuclear security managers need to think carefully about the incentives employees face, and work to make sure that the incentives point in the direction of good security performance rather than poor security performance.

One element of getting incentives pointed in the right direction is to do away with unneeded security rules—rules that are overly burdensome or complex and that contribute little to the overall security of the plant. When employees encounter rules they think are senseless, they typically do not comply with them. This can contribute to a broader culture in which people follow security rules only when they find it convenient, and they come to think of security as a problem for "them" and not "us." Every high-security organization has some of these unneeded or overly complex rules, as more rules get added over time in response to each incident that arises. By one estimate, "[i]n any large organization, *at least* 30% of the security rules, policies, and procedures are pointless, absurd, ineffective, or actually undermine security (by wasting energy and resources, by creating cynicism about security, and/or by driving behaviors that were not anticipated)."[49] Organizations should have regular processes to search for such rules and get rid of them.

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

Some of the highest consequence threats that security organizations face are from malicious outsiders: for intelligence agencies this means an adversary's spies; for military units, it is enemy forces; for nuclear facilities, it is thieves and saboteurs. Security organizations may therefore focus on preventing attacks or theft by outsiders, and to the degree that they protect against insider threats, they focus on the danger that individuals inside the organization might be recruited by or become sympathetic to a malicious outsider group—hence the attention paid to preventing "penetration" through counterintelligence and personnel screening and monitoring.

48. U.S. Department of Energy, Office of the Inspector General, *Inspection Report: Protective Force Performance Test Improprieties*, DOE/IG-0636 (Washington, D.C.: DOE, January, 2004); http://energy.gov/ig/downloads/inspection-report-protective-force-performance-test-improprieties-doeig-0636.

49. Johnston, "Mitigating the Insider Threat (and Other Security Issues)."

Yet this focus ignores the possibility that an insider threat can occur when an individual commits a dangerous act, not out of malicious intent, but for other complex reasons. The official definitions of insider threats in the IAEA guidelines encourage this focus because they emphasize the malicious characteristic of such a threat. The first definition introduced is of the term "adversary," which is described as "any individual performing or attempting to perform a malicious act."[50] The IAEA definition of "insider" builds on this definition of adversary: "The term 'insider' is used to describe an adversary with authorized access to a nuclear facility, a transport operation or sensitive information."[51] Thus, both definitions include a component of malice. The IAEA definition of a threat also implies the presence of malicious intent: "The term 'threat' is used to describe a likely cause of harm to people, damage to property or harm to the environment by an individual or individuals with the motivation, intention and capability to commit a malicious act."[52] But individuals who plausibly had no malicious intent even though they had very faulty, even horrific, judgment have caused serious insider threat incidents.

The October 2001 U.S. anthrax attacks, in which at least five letters containing anthrax spores were mailed to reporters and political figures, provide a dramatic case in point—though one where the errors of judgment were so extreme as to edge into the territory covered by the IAEA's definitions. As a result of these mailings, at least twenty-two victims contracted anthrax, five people died, thirty-five postal facilities were contaminated, and the presence of the anthrax spores was found in seven buildings on Capitol Hill.[53] But it appears that there may have been no real intent to kill or sicken anyone. The best available evidence suggests that Bruce Ivins, a senior scientist at the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID), mailed the envelopes along with letters declaring "Death to America . . . Allah is Great." Ivins was not, however, sympathetic with al-Qaeda, and it is believed that his main motive was to renew national interest in the threat of anthrax. Ronald Schouten, in the *Harvard Review of Psychiatry*, lists Ivins's motives as "an effort to enhance the profile of his anthrax work, to improve his own standing among colleagues, and to stimulate funding for biodefense by inducing fear in the population and influencing government policy."[54]

50. International Atomic Energy Agency, "Preventive and Protective Measures against Insider Threats" (Vienna: IAEA, September 2008), http://www-pub.iaea.org/MTCD/publications/PDF/pub1359_web.pdf (accessed May 17, 2013).

51. Ibid.

52. Ibid.

53. U.S. Department of Justice, "Amerithrax Investigative Summary," February 19, 2010, http://www.justice.gov/amerithrax/docs/amx-investigative-summary.pdf (accessed May 17, 2013).

54. Ronald Schouten, "Terrorism and the Behavioral Sciences," *Harvard Review of Psychiatry* 18 (6) (2010): 370.

Personal motives were certainly mixed up with the national security motive: Ivins had been a major contributor to the development of a controversial anthrax vaccine, and a terrorist anthrax attack had the potential to make his work more relevant, increase the patent-related fees that he was receiving, and impress a woman with whom he worked.[55] In retrospect, Ivins was clearly a sick man with warped judgment and a reckless willingness to risk the lives of others, but he did not intend to kill many people through his anthrax mailings. Had he intended to do so, the likely death toll would have been much larger.

Many other examples of "nonmalicious" but highly misguided insiders could be cited: Wen Ho Lee, who, if his version of events is correct, took highly classified information home as a backup system to make consulting work easier after leaving the Los Alamos Laboratory; Oleg Savchuk, who allegedly placed a virus into the computer control system at the Ignalina Nuclear Power Plant in order to call attention to the need for improved security and to be rewarded for his diligence; or John Deutch, the CIA director who handled highly sensitive classified information on an insecure computer connected to the Internet.[56] Indeed, security problems arising through inadvertence, conflicting incentives, and poor judgment are so pervasive that one U.S. security expert concluded: "The insider threat from careless or complacent employees and contractors exceeds the threat from malicious insiders (though the latter is not negligible). . . . This is partially, though not totally, due to the fact that careless or complacent insiders often unintentionally help nefarious outsiders."[57]

The lesson that should be learned from these incidents is that efforts to prevent insider threats primarily through screening for loyalty or, conversely, monitoring for ties to malicious terrorist or criminal organizations are insufficient. Such methods will not detect or deter individuals who make poor judgments, even radically poor judgments, in the name of a private interest or even in pursuit of a distorted vision of the public good. Nuclear security managers need to focus on the nonmalicious sources of insecurity as well. Building a strong security culture and making good security convenient are two places to start.

55. U.S. Department of Justice, "Amerithrax Investigative Summary"; David Willman, *The Mirage Man: Bruce Ivins, the Anthrax Attacks, and America's Rush to War* (New York: Bantam, 2011), 190; and Jeanne Guillemin, *American Anthrax* (New York: Times Books, 2011), 131.

56. Wen Ho Lee and Helen Zia, *My Country Versus Me* (New York: Hyperion, 2001); William Potter and Charles Ferguson, *The Four Faces of Nuclear Terrorism* (New York: Routledge, 2005), 224; and Central Intelligence Agency Inspector General, *Report of Investigation: Improper Handling of Classified Information by John M. Deutch*, 1998-0028-IG (Washington, D.C.: CIA, February 18, 2000). Lee was indicted for stealing classified nuclear weapons designs to share with China, though this has never been proven to the satisfaction of a court. The judge in the case ultimately apologized to Lee for his treatment.

57. Johnston, *Security Maxims.*

Lesson #10: Don't Focus Only on Prevention and Miss Opportunities for Mitigation

The IAEA's best practices guide for insider threats clearly recognizes the need to maintain both rigorous prevention programs and serious mitigation preparations as part of any nuclear security program. Indeed, even the title of the guide, *Preventive and Protective Measures against Insider Threats*, highlights that need. Yet there can be a strong temptation to favor prevention efforts over mitigation efforts, especially when dealing with exercises in which the public is involved, in order to avoid public fears that security incidents are likely.

Although the 2011 Fukushima accident is clearly a safety, not security, incident, it highlights the dangers that can be created when operators and officials avoid practicing mitigation and emergency response preparations in order to enhance public support for nuclear power and prevent panic. Yoichi Funabashi and Kay Kitazawa have compellingly identified a dangerous "myth of absolute safety" that was used to promote confidence in accident prevention measures, rather than conduct nuclear emergency response activities in Japan prior to the March 2011 accident. As Funabashi and Kitazawa explain:

> This myth [of absolute safety] has been propagated by interest groups seeking to gain broad acceptance for nuclear power: A public relations effort on behalf of the absolute safety of nuclear power was deemed necessary to overcome the strong anti-nuclear sentiments connected to the atomic bombings of Hiroshima and Nagasaki. . . . One example of the power of the safety myth involves disaster drills. In 2010, the Niigata Prefecture, where the 2007 Chuetsu offshore earthquake temporarily shut down the Kashiwazaki-Kariwa Nuclear Power Plant, made plans to conduct a joint earthquake and nuclear disaster drill. But NISA (the Nuclear and Industrial Safety Agency) advised that a nuclear accident drill premised on an earthquake would cause unnecessary anxiety and misunderstanding among residents. The prefecture instead conducted a joint drill premised on heavy snow.[58]

The myth that the facilities were absolutely safe was repeated so often that it affected operators' thinking about emergency response. The accident response plan for the Fukushima Daiichi site reportedly said, "The possibility of a severe accident occurring is so small that from an engineering standpoint, it is practically unthinkable." If that is what you believe, you are not likely to put much effort into preparing to mitigate severe accidents—and they did not.[59]

Fortunately, important steps can be taken to mitigate both sabotage and theft at nuclear facilities. The key steps to mitigate severe sabotage are largely the same as the key steps to mitigate severe accidents: making sure that electric

58. Yoichi Funabashi and Kay Kitazawa, "Fukushima in Review: A Complex Disaster, a Disastrous Response," *Bulletin of the Atomic Scientists* 68 (March/April 2012): 13–14.

59. Phred Dvorak and Peter Landers, "Japanese Plant Had Barebones Risk Plan," *The Wall Street Journal*, March 31, 2011.

power can be rapidly restored, that the reactor core and the fuel in the spent fuel pool can always be kept under water, and that if radioactivity *is* released from the core, the amount released to the environment can be limited.

With respect to nuclear material theft, mitigation steps are less effective, for once nuclear material has left the site where it is supposed to be, it could be anywhere; the subsequent lines of defense are largely variations on looking for a needle in a haystack. Nevertheless, relatively simple steps toward mitigation should not be neglected. In recent years, for example, the U.S. government has been pressing for countries to ship plutonium and HEU in forms that would require some chemical processing before they could be used in a bomb, rather than in pure form. Various elements of the effort to interdict nuclear smuggling can also be thought of as mitigation steps should nuclear theft prevention efforts fail.

But the Fukushima case makes clear that it is important to avoid, in both public presentations and private beliefs, the "myth of absolute security." The belief that a facility is already completely secure is never correct—and will lead to complacency that is the enemy of preparedness for either prevention or mitigation. Prevention of insider threats is a high priority, but leaders and operators should never succumb to the temptation to minimize emergency response and mitigation efforts in order to maintain the illusion that there is nothing to be afraid of.

THE PATH FORWARD

Even this brief comparative look at insider threats illustrates that such threats come in diverse and complex forms, that the individuals involved can have multiple complex motives, and that common, though understandable, organizational imperfections make insider threats a difficult problem to address adequately. Most nuclear organizations appear to underestimate both the scale of the insider threat and the difficulty of addressing it. Serious insider threats may well be rare in nuclear security, but given the scale of the potential consequences, it is crucial to do everything reasonably practical to address them.

The main lesson of all these cases is: do not assume, always assess—and assess (and test) as realistically as possible. Unfortunately, realistic testing of how well insider protections work in practice is very difficult; genuinely realistic tests could compromise safety or put testers at risk, while tests that security personnel and other staff know are taking place do not genuinely test the performance of the system. Nevertheless, nuclear security managers need to establish programs for assessment and testing that are as creative and realistic as practicable—and to reward the employees involved for finding vulnerabilities and proposing ways to fix them, rather than marginalizing people who complain about security vulnerabilities. Ensuring that all operators handling nuclear weapons, weapons-usable nuclear materials, or nuclear facilities whose sabotage could have catastrophic consequences have genuinely effective measures in place to cope with insider threats should be a major focus of the nuclear security summit process, of the

IAEA's nuclear security efforts, of WINS's nuclear security program, and of regulatory and industry efforts around the world.

Complacency—the belief that the threat is modest and the measures already in place are adequate—is the principal enemy of action. Hence, a better understanding of the reality of the threat is critical to getting countries around the world to put stronger protections in place.

To foster such an understanding, we recommend that countries work together to establish shared analyses of incidents and lessons learned. In the world of nuclear safety, when an incident occurs, the plant performs a root-cause analysis and develops lessons learned to prevent similar incidents from occurring again. These incident reports and lessons learned are then shared with other reactor operators through organizations such as WANO and national groups such as the U.S. Institute of Nuclear Power Operations (INPO). These organizations can then assess trends among the incidents. INPO not only distributes lessons learned to U.S. reactor operators, it carries out inspections to assess how well reactor operators are implementing lessons learned. Nothing remotely resembling this approach exists in the nuclear security world. It is time to begin such an effort—assessing security-related incidents in depth, exploring lessons learned, and distributing as much of this information among nuclear security operators as necessary secrecy will allow. As we have done in this paper, the analyses should include non-nuclear incidents that reveal types of problems that arise and types of tactics against which nuclear materials and facilities should be protected. Information about incidents and how to protect against them could be a major driver of nuclear security improvement, as it has been in safety; in a recent survey of nuclear security experts in eighteen countries with weapons-usable nuclear material, incidents were cited far more often than any other factor as a dominant or very important driver of countries' recent changes in nuclear security policies.[60] States could begin with internal assessments of events within their territory, and then provide as much information as possible to an international collection of facts and findings.

Overall, there is a need for more in-depth, empirically grounded research on insider threats to nuclear security and what works best in protecting against them. Such research focused on cybersecurity is beginning to become available, but genuinely empirical work on nuclear security is in its infancy. Fortunately, only a modest number of serious insider cases have been identified in the nuclear world. Unfortunately, it is likely, given the classified nature of security records and reports, that we have not identified all serious cases of insider threats from the past. Moreover, the potential danger is so high in the nuclear world that even a modest number of insider incidents is alarming. There is much research and analysis to be done—and action to be taken. This paper is only a beginning, not an end.

60. Bunn and Harrell, *Threat Perceptions and Drivers of Change in Nuclear Security Around the World*, http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf.

Contributors

Matthew Bunn is Professor of Practice at the Harvard Kennedy School. His research interests include nuclear theft and terrorism; nuclear proliferation and measures to control it; the future of nuclear energy and its fuel cycle; and innovation in energy technologies. Before coming to Harvard, he served as an adviser to the White House Office of Science and Technology Policy, as a study director at the National Academy of Sciences, and as editor of *Arms Control Today*. He is the author or coauthor of more than 20 books or major technical reports (most recently *Transforming U.S. Energy Innovation)*, and over a hundred articles in publications ranging from *Science* to *The Washington Post*.

Scott D. Sagan is the Caroline S.G. Munro Professor of Political Science and Senior Fellow at the Center for International Security and Cooperation at Stanford University. He is a Fellow of the American Academy of Arts and Sciences and Cochair of the Academy's Global Nuclear Future Initiative. He is the author of, among other works, *The Limits of Safety: Organizations, Accidents, and Nuclear Weapons* (1993) and *The Spread of Nuclear Weapons: An Enduring Debate* (with Kenneth N. Waltz, 2012).

American Academy of Arts and Sciences

Selected Publications of the American Academy

The Back-End of the Nuclear Fuel Cycle: An Innovative Storage Concept
Stephen M. Goldberg, Robert Rosner, and James P. Malone

Multinational Approaches to the Nuclear Fuel Cycle
Charles McCombie and Thomas Isaacs, Noramly Bin Muslim, Tariq Rauf, Atsuyuki Suzuki, Frank von Hippel, and Ellen Tauscher

Nuclear Collisions: Discord, Reform & the Nuclear Nonproliferation Regime
Steven E. Miller, Wael Al-Assad, Jayantha Dhanapala, C. Raja Mohan, and Ta Minh Tuan

Game Changers for Nuclear Energy
Kate Marvel and Michael May

Nuclear Reactors: Generation to Generation
Stephen M. Goldberg and Robert Rosner

Shared Responsibilities for Nuclear Disarmament: A Global Debate
Scott D. Sagan, James M. Acton, Jayantha Dhanapala, Mustafa Kibaroglu, Harald Müller, Yukio Satoh, Mohamed I. Shaker, and Achilles Zaluar

"On the Global Nuclear Future," vols. 1–2, *Daedalus*, 2009–2010

Science and the Educated American: A Core Component of Liberal Education
Edited by Jerrold Meinwald and John G. Hildebrand

Do Scientists Understand the Public?
Chris Mooney

To order any of these publications please contact the Academy's Publications Office.
Telephone: 617-576-5085; Fax: 617-576-5088; Email: publications@amacad.org

AMERICAN ACADEMY OF ARTS & SCIENCES