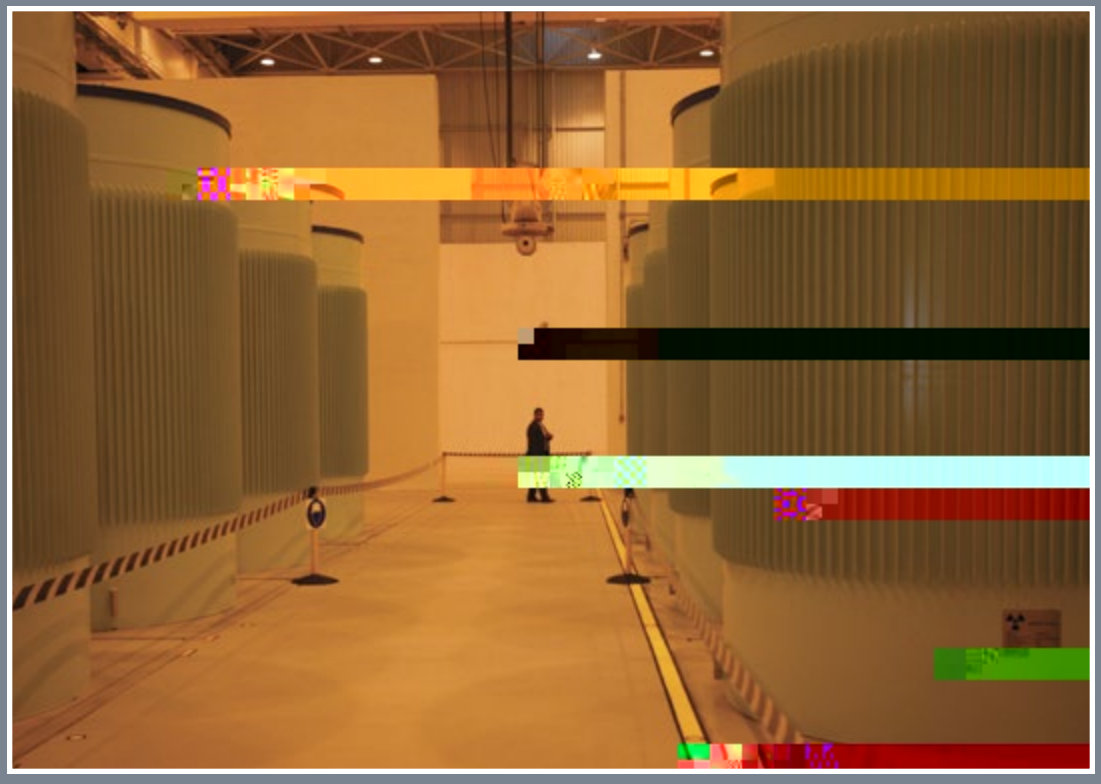
A Worst Practices Guide to Insider Threats: Lessons from Past Mistakes



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 [illegible]*, (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 *P , , I , , N , , , , : E , G E , *, 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," *E , D* , 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)," *M & G* (South Africa), December 15, 1995. Beresford has offered a more detailed account, based on interviews with the perpetrator, in , , , *F , : A D J , , , A , ,* (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,(nat( )]TJ0 Tc 0 Thsdy 1.34)]TJd03-

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 , 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

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

LESSONS

L #1: D ', A , , , , I , P , , NIMO (N , I M O ⌐ ,)

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," , *A* 24 (4) (2004): 935–946.

7. Ritu Sarin, , *A* , *I* *G* (New Delhi: Penguin, 1990), 19.

8. Ibid.

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: caheft

L #3: D ', A , , , , F , , P ,

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,

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.

L #4: D ' A I C I

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.

L #5: D ' P M

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, *B D C N A :* (Cambridge, Mass.: Project on Managing the Atom, Harvard Kennedy School, March 2014), http://belfercenter.ksg.harvard.edu/files/surveypaperfulltext.pdf.

28. Hoffman et al., *I C*.

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," *I A - A*, 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," *K D*, 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 con-

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

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.

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

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."

L #8: D ' A F

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, "*B P* " *I I* .

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

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 *H , , P , ,* , 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," *H , , P , -* , 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, *M , M : B , I , , A , A , , , A , ' ,* (New York: Bantam, 2011), 190; and Jeanne Guillemin, *A , , A ,* (New York: Times Books, 2011), 131.

56. Wen Ho Lee and Helen Zia, *M C , , M* (New York: Hyperion, 2001); William Potter and Charles Ferguson, *, F F, N , ,* (New York: Routledge, 2005), 224; and Central Intelligence Agency Inspector General, *, , I , , , : I , H C f, I , J M. D , ,* 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, *, , M* .

L #10: D ', F O P, , , M O , ,, M , ,

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, *P, , , , P , , , M , , I , , ,*, 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.

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 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 ade-

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, , , P , , D , C , N , , , A , , , 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 *A C* . He is the author or coauthor of more than 20 books or major technical reports (most recently . . *E* , *I* ,), and over a hundred articles in publications ranging from , , , to , , *P* ,.

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, , *L* , , , : *O* , *A* , , , *N* , , (1993) and , , *N* , , *: A E D* , (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 Of ce.
Telephone: 617-576-5085; Fax: 617-576-5088; Email: publications@amacad.org

AMERICAN ACADEMY OF ARTS & SCIENCES