Preventing Insider Theft: Lessons from the Casino and Pharmaceutical Industries

Matthew Bunn
Harvard Kennedy School, Cambridge, Massachusetts USA

Kathryn M. Glynn
IBM Global Business Services, Herndon, Virginia USA

Abstract

Through structured interviews and a literature review, we assess which approaches to protection against insider thefts in the casino and pharmaceutical industries could be usefully applied to strengthen protections against insider theft in the nuclear industry, where insider thefts could have very high consequences. Among other measures, we suggest consideration of constant video surveillance of all vaults and insider-material interactions; frequent and rigorous material accounting; requiring everyone who touches material to sign for it; implementing an expanded two-person rule; rewarding attention to security; and establishing incident databases and experience sharing. While many of these measures are in place for some operations with weapons-usable material in some countries, they should be considered for more universal application.

Introduction

At the Washington nuclear security summit in April 2010, leaders from some forty-seven countries affirmed that "nuclear terrorism is one of the most challenging threats to international security, and strong nuclear security measures are the most effective means to prevent terrorists, criminals, or other unauthorized actors from acquiring nuclear materials."[1] The leaders reaffirmed their commitment to take action to improve nuclear security at the Seoul nuclear security summit in March 2012.[2]

Nearly all of the documented thefts of highly enriched uranium (HEU) or separated plutonium—the two materials that could be used to make a nuclear bomb—appear to have been perpetrated by insiders. Protection against insider threats, therefore, is an absolutely critical element of keeping the essential ingredients of nuclear bombs out of terrorist and criminal hands. Insiders, with their authorized access to sensitive areas and materials, their knowledge of the nuclear security system and its weaknesses, and their relations with other staff, pose major challenges for security planners.

To address this threat, a broad range of insider protection measures are required in national regulations and recommended in international guidelines for handling weapons-usable nuclear material (and, often, for operations in vital areas of nuclear facilities as well), including checks to ensure insiders are trustworthy before granting access; two-person or three-person rule, so that no one is alone with weapons-usable nuclear material; continuous surveillance of material operations; searches on entering and leaving key areas; accounting sufficiently accurate to detect either abrupt or protracted thefts; use of uniquely identifiable and difficult-to-defeat tamper-indicating devices; and storage of material in secure vaults or vault-type rooms when not in use.[3] A number of useful sets of recommendations for protecting against insider theft of nuclear material have been developed.[4]

Nevertheless, insider-threat protection practices in the nuclear industry vary widely, and are often focused on simply complying with national-level rules, rather than focusing on continuous performance improvement. In this article, we explore practices for protecting against insider threats in two high-security industries with a profit incentive to achieve excellence in preventing insider theft—casinos and controlled pharmaceutical production—and explore whether the nuclear industry can adapt practices from these industries.[5]

To perform our assessment, one of us carried out structured interviews with security managers for several casinos and pharmaceutical facilities producing drugs with high black-market value. The interviews were based on a consistent set of questions, for comparability from one interview to the next, but also flexibly pursued issues as they arose in the discussions. Because of limitations of time and resources, these interviews covered only a limited number of facilities, and covered only facilities located in the United States. All of the interviewees wished to remain anonymous, and to keep the facilities whose security they managed unnamed as well. We combined these interviews with a review of relevant literature on casino and pharmaceutical security;[6] a review of literature on nuclear industry practices to protect against insiders (such as the material already cited); and extensive discussions with nuclear industry experts on insider protection by one of the authors over a period of several years.

Our assessment is that both the casino and pharmaceutical industries have developed some valuable approaches that the nuclear industry should consider adopting. While many of

the practices we consider are already in use for operations with weapons-usable materials in some countries, they should be considered for broader application. At the same time, the casino and pharmaceutical industries are different from the nuclear industry in some key respects. In particular, both industries accept that in some cases the expense of preventing small thefts may not be worth the cost of prevention—an attitude those handing weapons-usable nuclear material cannot afford to adopt when it comes to kilogram quantities of weapons-usable material.

We proceed in several stages. First, we offer a framework for analyzing programs to protect against insider theft, dividing these into categories. Second, we describe the insider protections used in the casino and the pharmaceutical industries, using this framework. Third, we offer recommendations for the nuclear industry, intended to supplement best-practice guidance documents that have already been developed, on which we also draw.

Insider Protection: A Framework for Analysis

All situations involving protection against potential insider threats involve some combination of managing the potential insiders and managing the items to be protected (which might be things that might be stolen, areas of a facility that might be sabotaged, people who might be attacked, or information that might be stolen, damaged, or misused).

For this analysis, which focuses on items or materials that might be stolen, we refer to the items to be protected as "critical material," and we identify two kinds of information we refer to as "critical knowledge." First-degree critical knowledge, such as vault combinations, is knowledge that provides a major step toward gaining direct access to critical material. Second-degree critical knowledge can be characterized as security-related knowledge that conscientious employees should ideally bring to the attention of management or of security personnel, but that, if it remains concealed or forgotten rather than reported, increases the ease of diversion.[7] Examples of second-degree critical knowledge include the location of a blind spot in an area supposedly monitored by a surveillance camera, or the insight that a colleague has been rendered a target for blackmail by financial or personal difficulties.

Programs to protect against insider threats generally combine elements addressing the following six questions, with varying degrees of emphasis:

1. *How are insiders screened and monitored to ensure they are trustworthy?*

Most high-security organizations perform some form of background check before giving people access to items, areas, or information to be protected, or information about how these are secured. The thoroughness of such checks varies widely, ranging from a simple criminal background check (or less) to a full investigation, in which the person's career, financial status, mental health, friends, and family are all considered. Some form of monitoring of authorized insiders may be continued after they are employed, to detect notable changes in behavior or circumstances that may bear on their propensity to become an insider. (Many accounts of insider cases note that they are often preceded by inappropriate behaviors noticed by coworkers.[8]) In many environments, for example, insiders must undergo new background checks every few years to maintain their clearance, and staff are encouraged to report any changes in their own circumstances or suspicions about others. Both initial background screening and ongoing monitoring of employee behavior raise issues of privacy and civil liberties, and how much intrusion employees agree to permit varies depending on whether they are joining, for example, a highly secretive intelligence agency or a commercial company not dealing with anything relating to the national security.

2. *How are staff trained and motivated to reduce their vulnerability to becoming insiders and to convince them to watch for and report suspicious activities or security weaknesses?*

Keeping up staff morale and motivation, and convincing them to be active participants in achieving good security, are critical elements of an effective program to protect against insiders. One obvious step is ensuring that staff are adequately paid, so that desperation and anger at the organization for undervaluing them do not add to the motivation for insider theft.[9] Programs to make employees feel that they are well-treated and their concerns are addressed are also important, and need not be particularly expensive. Studies of insider theft and sabotage in non-nuclear industries regularly conclude that simple employee disgruntlement is a major contributing factor.[9]

Many organizations use training and incentives programs to convince employees to take security seriously, be on the lookout for insider dangers, and report any suspicious activity or security weaknesses requiring correction that they observe. Many organizations also provide training to employees to recognize and counter efforts to recruit them for nefarious purposes (for example counter-intelligence briefings that are often given to people with authorized access to secret information).

Particularly difficult issues arise when authorized employees know they are about to lose their jobs, or have just left their jobs. At these moments, the organization's ability to offer incentives and disincentives is much reduced and the employees' loyalty to the organization may be minimal, yet their access to critical materials or knowledge that could facilitate a malevolent act may remain unchecked. Our interviews suggest that nsider programs often include steps for dealing with these kinds of situations, such as removing employees from the most sensitive forms of access once they are in the process of leaving the organization, changing keys, combinations, or passwords after an employee with access to them has left, and making clear the penalties associated with providing key information to unauthorized individuals after employment. In some cases, some monitoring of employees' ac-

Figure 1. Forms of monitoring, control, and incentives

tivities continues for some time after access is terminated. The passports of Russian nuclear weapons designers, for example, are reportedly held in the safe of the site security officer for five years after their employment comes to an end.[10]

Figure 1 summarizes the different forms of monitoring, control, and incentives and disincentives that may be applied at each stage of the employee life-cycle.

3. *How are the items to be protected controlled, monitored, and accounted for?*

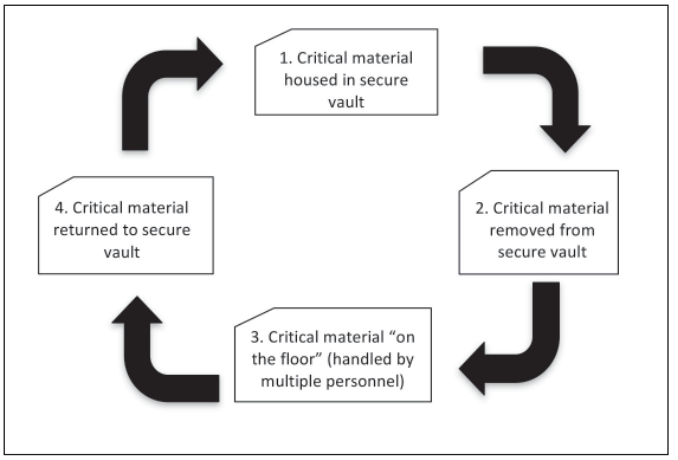
Methods to secure and control the protected items themselves vary widely, depending on the circumstances of particular industries and operations. At Fort Knox, at one extreme, gold bars virtually never leave hardened vaults, and virtually no one ever enters those vaults. At the other extreme, in a casino, money and chips that can be exchanged for money are constantly handled in large quantities by hundreds of people on the gaming floor. Virtually all high-security organizations, however, will have some element of security, monitoring, and accounting for the items, areas, or information they are trying to protect. In particular, monitoring measures such as security cameras can make it possible to detect thefts as they are occurring, and accurate accounting can make it possible to confirm that nothing significant is missing—or to identify when things *do* appear to be missing and further investigation is required.

Items likely to tempt thieves due to their high value, portability, and related characteristics often go through a regular cycle: storage in a secure vault when not in use, removal from the vault, processing and use on the equivalent of a "shop floor," and return to the vault. See Figure 2. The interviews conducted for this paper focused closely on how security is managed for each of the steps in this cycle, and how employees are screened, monitored, and motivated.

4. *How are interactions between the insiders and the items to be protected limited and monitored?*

Controlling who can have access to the critical material, under what circumstances, is often among the most important elements of a program to protect against insider threats. In many

Figure 2. Generic critical material cycle



organizations, for example, no one would be allowed to access the critical material without a clear job requirement to do so; protected items might be kept in a vault when not in use, with very few people having authorized access to the vault; a two-person rule might be in place, prohibiting anyone from being alone with the material; and security cameras might provide additional monitoring whenever items are accessed.

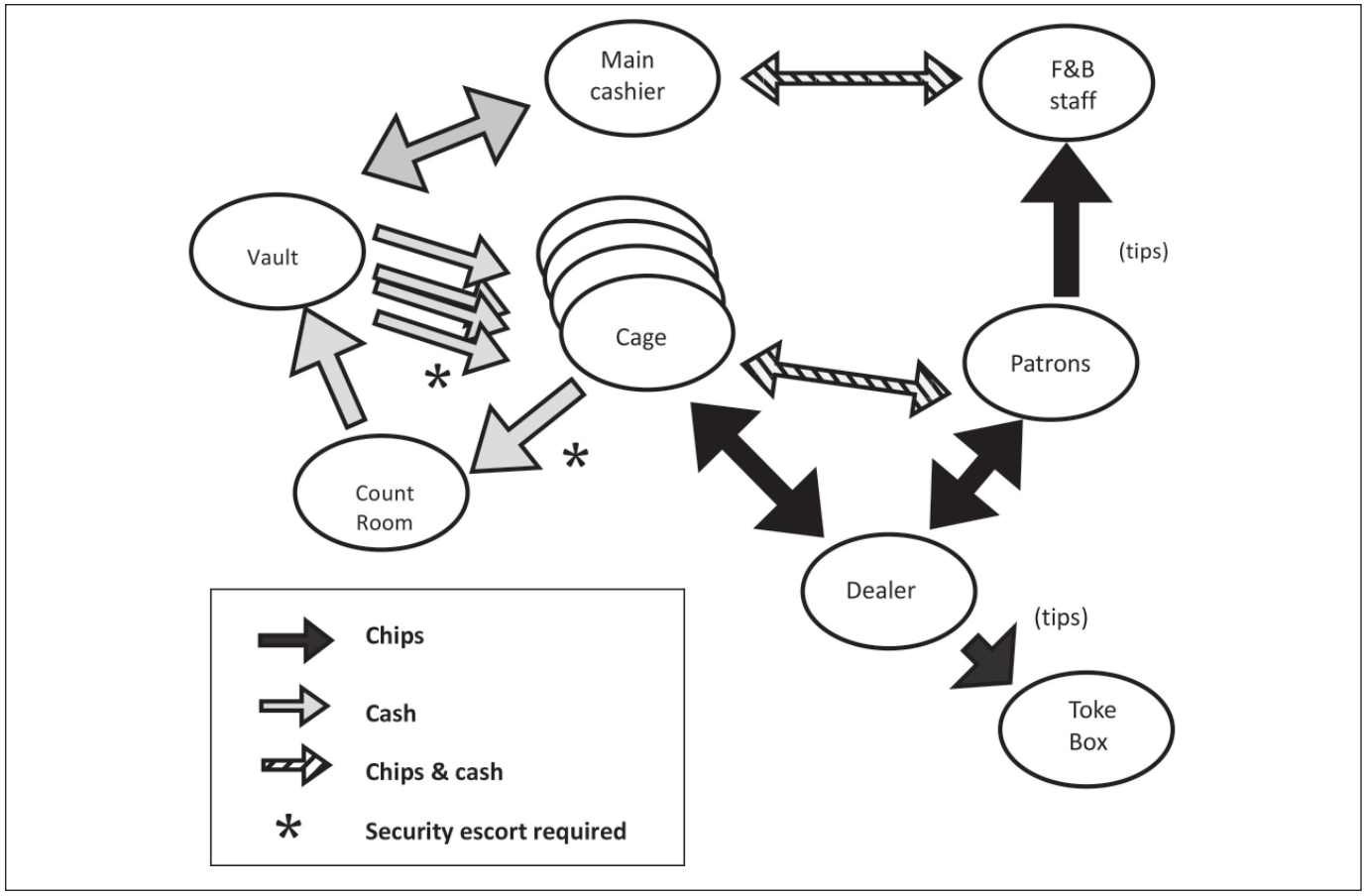
5. *How are investigations done to find insiders that may exist?*

Despite their best efforts, organizations sometimes find they have a malevolent insider in their midst—a thief, a saboteur, an assassin, a spy. Sometimes only indirect evidence exists that hints at this possibility. Many high-security organizations have processes for investigating the possibility of insiders in their midst. In some cases, this can be done discretely, with little disruption to the organization. There are other cases, however, where the hunt for an insider can lead to major impacts on morale, with everyone suspecting everyone else.

6. *How are testing, assessment, and learning from experience done?*

Security systems must be assessed to see how effective they are. Some organizations use a "red teaming" approach, in which small

Figure 3. Gaming critical material flow



groups are charged with examining the security measures in place and trying to conceive of ways to overcome them. Often particular elements of the system are subject to tests, such as how accurate the accounting of material is or whether an alarm sounds when material is carried past certain detectors or a vault is opened without proper authorization. Mechanisms for learning from past experience of what does and does not work are also important.

Having laid out this framework, we will now discuss security against insiders in the casino and pharmaceutical industries in the United States, examining how each of these six elements is implemented in these two industries, and how much reliance is placed on each. In each case, we will begin by describing the general environment in the industry in question, which can have a major bearing on protection against insider threats.

Protection Against Insider Theft in the Casino Industry

Environment, Operations, and Security Assumptions

The critical material in a casino is cash and chips. Chips are used at gaming tables, and patrons can exchange them for cash at cages located throughout the gaming floor, or at the main cashier. Employees can only exchange chips they may receive as tips at the main cashier. When not in use at the cages or the main cashier, cash is stored in a secure vault, and counted in a special "count room," which is a vault of its own. See Figure 3. The use of chips rather than cash is itself an anti-theft measure, as the chips have no inherent value and are less likely than cash to be targeted by casual thieves.[11]

In principle, the cash and chips in a casino are individual countable items, but they are so numerous as to make frequent item-by-item accounting difficult. In this respect, a casino is somewhat analogous to a nuclear facility handling large numbers of small items, such as a facility assembling pellets or plates of nuclear material into fabricated fuel elements, where critical nuclear materials would be removed from a secure vault and accounted for before and after their use on the floor.

Casinos are a customer-facing industry and cannot allow security measures to encroach on the customer experience. Thousands of people enter and leave the casino every day carrying both chips and cash, and because the casinos seek to maintain a welcoming atmosphere for customers, the security personnel do not search or scan them.

For gaming establishments, the motivation to ensure against the diversion of critical materials is purely financial. Small-scale diversions are typically not considered worth the time, effort and money required to stop them. Gaming security managers reported that a cashier could probably skim "a few hundred dollars" a day without detection.

Our interviews indicate that security professionals in the gaming industry operate under two unique assumptions. First, they assume that some threat, internal or external, is *always* present. Second, casino security professionals assume that non-security staff (dealers, waitresses, cashiers, and so on) are probably *not* trustworthy, and may well prove to be thieves. To paraphrase one interviewee, "If I never hired anyone with a questionable personal history, I'd have to turn down 90 percent of the job applicants in Vegas."

The casino security managers who participated in our study indicated that regulations governing the casino industry typically require that the security operation be composed of two distinct and independent units. *Security* staff members are a visible presence on the floor. They are trained in customer relations as well as security procedures and are charged with maintaining the physical security of the casino. *Surveillance* team members sit in secluded rooms monitoring security camera feeds from throughout the casino. Every table game is monitored from multiple angles to identify cheaters. Surveillance teams typically verify employee ID badges for access into secure areas, and monitor the vault interiors and doors, cages, and the "count room"—a separate vault where the money is counted. Cameras are carefully hidden so that patrons do not feel like they are being spied on. Employees, on the other hand, always know that "Big Brother" is watching. To address the possibility of the casino's general manager being involved in activities he or she might wish to cover up, the surveillance team reports to a distinct chain of command, not through the general manager.

Screening and Monitoring Staff

Most floor employees are hired at the entry level and are given little responsibility for or access to first-degree critical knowledge. Nevertheless, employment applications include authorization to conduct a criminal background check and a credit check. Red flags would include major property crime or fraud arrests, gambling addictions, or significant debt (though two managers indicated that the 2008 financial meltdown has made bankruptcy too common to be considered a red flag). Security and surveillance personnel undergo more stringent background checks, though nothing like the screening required for a security clearance to handle weapons-usable nuclear material.

Casinos do not specifically monitor changes in employee behavior off the job after hiring (such as sudden and unexplained wealth). On the job, suspicious changes in behavior may show up in surveillance. One interviewee reported a case in which a cocktail waitress began spending inordinate amounts of time near one particular gaming table; the casino eventually discovered that she was colluding with a dealer to steal chips.

Casinos also maintain a list of "permanently ejected" individuals. The "permanently ejected" list includes patrons that are banned from the premises for reasons varying from drunken brawls to gambling addiction, as well as former employees fired for misconduct or theft.

Security personnel escort employees terminated for cause off the property, and their ID and access badges are confiscated. Door codes (where they are utilized) are immediately changed. One casino reported that all ex-employees are banned from the premises for ninety days, while another indicated that they allow former employees to return as patrons as long as they were not placed on the "permanently ejected" list. Every casino security manager interviewed indicated that the processes and security and surveillance systems already in place could be relied upon to stop an ex-employee from abusing critical knowledge.

Training and Motivating Staff

Most new employees undergo approximately two days of orientation, primarily on casino operations. New hires are indoctrinated into the security operations specific to their own work. Security and surveillance personnel require more extensive training, which is also conducted on the job. Surveillance personnel are required to know how to play every table game, so that they can better detect cheats or card-readers, while security personnel are trained on how to conduct "chip counts," escort critical gaming materials, and interact with patrons.

Security and surveillance personnel often undergo weekly or monthly security training. Generally, training appears to be focused on procedures and practices rather than "red team" exercises (that is, exercises in which mock adversaries attempt to defeat the security system and the security team has to find ways to detect and respond to the attempt). In some instances, security training is just a part of a general training required by state regulations, including everything from sexual harassment prevention to security procedures. General floor employees receive regular security training only if a promotion requires additional access to critical materials or knowledge.

Floor employees make a reasonable wage when salary and tips are included. Security and surveillance personnel receive higher salaries because they do not receive tips. According to one casino security manager, wages are neither a major source of loyalty to the establishment nor a major source of disgruntlement.

All employees are aware that theft is an ever-present threat. Nevertheless, interviewees expressed the view that while security and surveillance staff were highly vigilant, general employees probably would not bother to report suspicious activity short of clear and overt misconduct. In some cases, the casinos provide training and other materials to emphasize to employees that threats to the casino's well-being are also threats to their jobs. But motivating non-security employees to be on the lookout for

security issues does not appear to be an area on which casinos place much emphasis. Multiple casino security managers, however, indicated that anonymous tip lines were one of their most productive security programs.

Controlling, Monitoring, and Accounting for Protected Items

Both a cashier and a security employee must agree to enter the vault where cash is secured. Cash and chip transfers between the vault and cages and between cages and tables require a security escort, dual concurrence, and signatures from both the deliverer and the receiver of the critical material, attesting to the accuracy of the count. At least every twenty-four hours, cash is collected from each cage and escorted to the count room. Dual concurrence is required to enter and exit the count room. To reduce the probability of collusion, a two-person team comprised of individuals from different organizations, typically a trained cashier and a Gaming Commission member, are present for the count. Surveillance cameras continuously monitor the interiors of and the entrances to the vault and the count room.

Limiting and Monitoring Insider-Item Interactions

Access to the vault, cages, and count room is permitted only to specified individuals under precise circumstances. Staff can only exchange the chips they receive for tips at the main cashier, where cashing an unusually large quantity or denomination of chips, or cashing-out unusually frequently, would raise questions. Dealers tips (also chips, which they are not allowed to cash) are placed in a locked toke box, located at every table, then distributed among dealers at the end of the week, based on the number of hours worked.

Uniforms for the floor staff are designed to discourage theft. Sleeves are typically elbow-length or shorter, and pockets are either disallowed or covered with an apron.

Conducting Investigations

Interviewees did not provide a great deal of detail about the investigations they conduct when a staff member is suspected of theft. Often suspicions are raised from, and key evidence provided by, activities observed on surveillance cameras.

Assessment, Testing, and Learning

Learning from collective experience, rather than formal testing and assessment, appears to be the mainstay of casino security operations. Casinos learn from problems they have encountered themselves, and also have a system for sharing information on threats. According to one source, a cheating ring was apprehended because casinos in New York, New Jersey, and Connecticut shared information including suspect descriptions and modus operandi. The first casinos hit were unable to stop the fraudsters, but were able to provide enough information to neighboring casinos that security and surveillance were able to identify and apprehend the offenders. Data sharing could provide similar results in cases of insider diversion schemes.

Potential Weak Points

Multiple security managers reported that dealers have been caught stealing chips, typically through sleight-of-hand. Dealers are prohibited from cashing chips, but a dealer-thief could easily collude with a food and beverage employee or a patron, who could cash the stolen chip without suspicion. Every casino reported surveillance as the primary method to detect and disrupt such a scheme.

Another potential vulnerability is cash-skimming from the vault, count room, or cage. One casino reported that cashiers who are either over or under on their cash-counts by a specified amount during a rolling twelve-month period are terminated. While the exact amount of acceptable gain or loss was not disclosed, a cashier with this second-degree critical knowledge could carefully steal just below the line and avoid detection–just as some nuclear material thieves have done.[12]

Finally, the standoffish relationship between surveillance and general employees has both positive and negative implications for diversion prevention efforts. Assuming that most employees are less than trustworthy, gaming security and surveillance officers are unlikely to suffer from the "halo effect," in which well-liked employees are assumed to be trustworthy.[13]

Constant awareness of being under surveillance and potential suspicion, however, is unlikely to generate feelings of loyalty or buy-in from most employees. Thus such approaches probably lower the threshold for individuals to cross over into illicit activity, and make employees less likely to report second-degree critical knowledge that could provide insight into potential security threats.

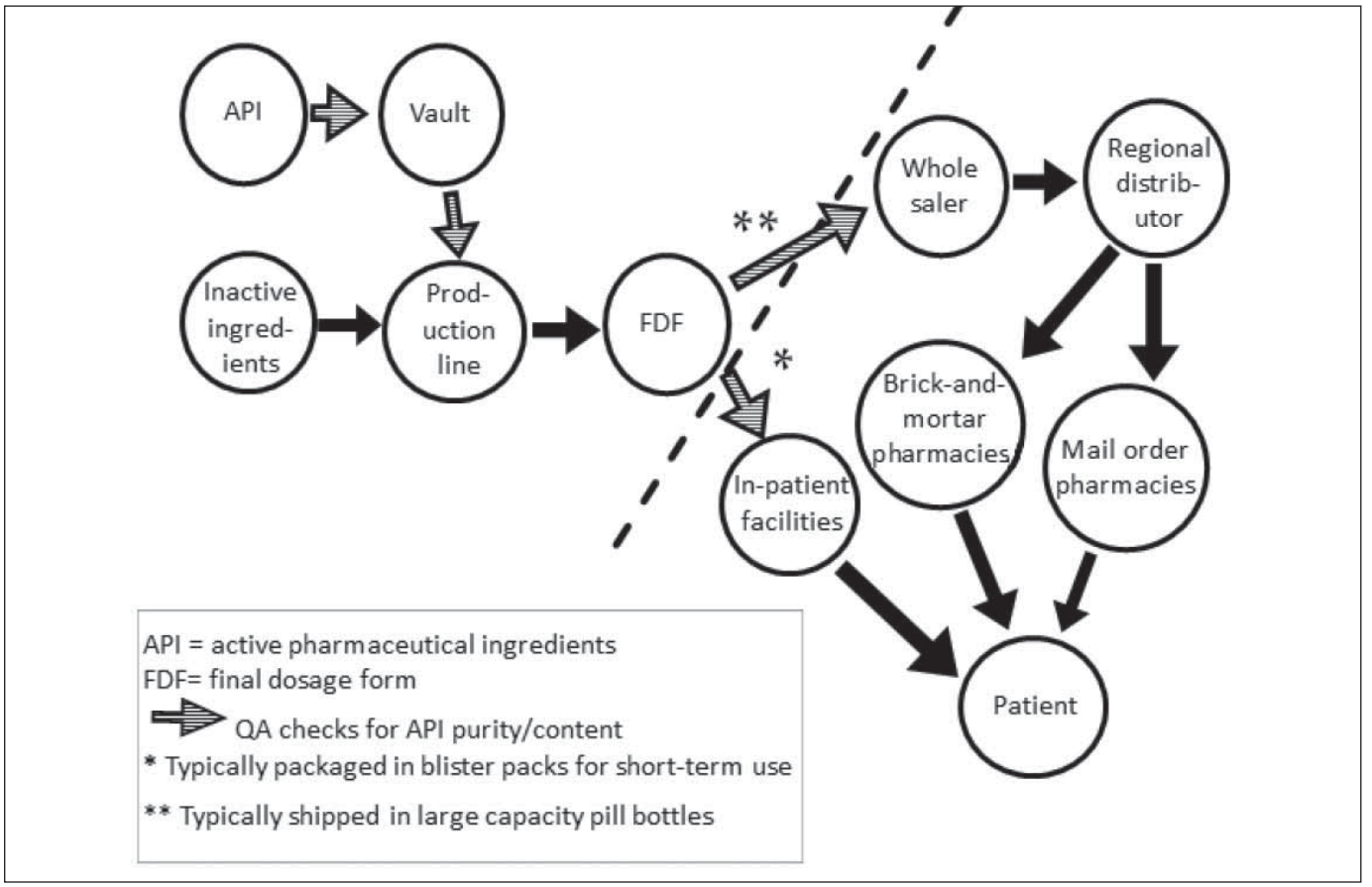
Protection Against Insider Theft in the Pharmaceutical Industry

Environment, Operations, and Security Assumptions

In this study, we focused on sites that produce and distribute a particular Schedule II narcotics (Schedule II are designated as controlled substances according to the U.S. Controlled Substance Act) that is subject to abuse and has a high street value. (Interviewees asked us not to specify which one, as only a few facilities produce it, and they did not wish to reveal facility-specific security information.) In these facilities, the active pharmaceutical ingredient (API) is stored in a secured vault until it is ready for use. It is then moved to the production area, where it is combined with inactive ingredients to make the final dosage form (FDF), small pills in the case of the facilities we focused on. The pills are then packaged and sent out to distributors, leaving the control of the original facility that made them. See Figure 4. Like a nuclear bulk-processing facility, these sites are producing or fabricating large quantities of critical material in bulk, and have to ensure that accounting uncertainties that suggest an operational gain or loss are not masking diversion.

Only a small portion of the security incentive in the pharmaceutical industry comes from the financial value of the drugs

Figure 4. Pharma critical material flow



that might be stolen; instead, companies want to avoid the brand impact of having their drugs driving black markets along with scrutiny (and potentially shutdown) from regulators. This means much lower tolerance for small-scale thefts.

The potential for insider theft exists at every level of the pharmaceutical production and distribution chain. Individuals employed at production sites, distribution centers, and pharmacies are all potential insiders. This study is based on interviews with security managers for production and distribution sites, and did not explore security at pharmacies or transporters handling these materials.

At the pharmaceutical distribution sites, most employees are professionally licensed pharmacists and pharmacy technicians, bound by the ethical standards of the American Pharmacists Association (APA), and keenly aware that a breach would result in the loss of their licenses. Interviewees assumed that APA licensing was a major contribution to reducing insider risks among these personnel, though it is not clear that this conclusion is backed by data. The pharmaceutical distribution site whose staff we interviewed did not differentiate between staff who did or did not handle controlled substances; but this facility trains surveillance cameras on every workstation at which controlled substances are handled. At production sites, staff are typically not licensed pharmacists or pharmacy technicians, but pharmaceutical producers reported requiring additional training and screening for individuals assigned to handle controlled substances in the factories.

The security managers we interviewed indicated that their operations, unlike casinos, do not differentiate between security and surveillance operations. Security personnel report to an on-site security manager, who in turn reports to the security manager at corporate headquarters. The site general manager is excluded from the security chain of command to maintain the objectivity and independence of the security operation. No regulations overtly restrict relationships between security and non-security staff, though according to one interviewee, they operate in "separate circles" that naturally limit daily interactions.

In addition to the security team, controlled substance teams (CSTs), usually comprised of security, compliance, and law-enforcement professionals, are assigned to every pharmaceutical production site handling Schedule II substances. Acting as something akin to an internal auditor, they are charged with ensuring that the company complies with both the letter and spirit of relevant regulations. Like the security team, the CSTs report to corporate headquarters rather than to site managers.

Security managers for controlled pharmaceutical producers report expending a great deal of effort to ensure security buy-in from corporate leadership on down. They attempt to ensure that every employee is aware of the harsh penalties for failing to comply with federal regulations. Simultaneously, pharmaceutical producers pride themselves as stewards of public health, and work to ensure that every employee shares that sense of responsibility. According to one interviewee, security has moved from being considered a "business disabler to a business enabler."

Quality assurance (QA) plays a central role in pharmaceutical production, and it is used as an element of theft prevention as well. At production sites, manufactured pills are pulled at random for QA checks. While these checks are primarily intended to ensure accurate formulation, they also provide a check against the diversion of API that would lead to detectable changes in pill formulation. At distribution sites, QA randomly selects filled prescriptions to check for the accuracy of pill-counts.

Producers and distributors of Schedule II substances are subject to several layers of regulation. The Drug Enforcement Administration (DEA) is the primary regulator concerned with theft of Schedule II pharmaceuticals. The DEA also regulates the design and construction of facilities producing or distributing controlled substances. The DEA approves blueprints for Schedule II production facilities to ensure compliance with security requirements. Though not required, many companies seek DEA guidance in designing their security system. The DEA has the authority to inspect facilities on short notice and can shut down a facility that is found to be in violation of security procedures.

The Department of Health and Human Services enforces the Health Insurance Portability and Accountability Act (HIPAA) of 1996, which guarantees privacy and security standards for patient information. Pharmaceutical distributors in particular appear to consider HIPAA training a valuable part of their employee indoctrination, and count on it to increase general security awareness and buy-in, though it is not focused on protecting against theft.

The Food and Drug Administration (FDA) is mainly concerned with quality assurance and regulatory compliance. The FDA would be the first regulator notified if QA detected an irregular formulation. Our interviewees indicated that most pharmaceutical distribution facility employees, and some staff at production sites, are licensed by the APA, and could lose their license if caught stealing or contributing to thefts by others.

Screening and Monitoring Staff

Pharmaceutical firms subject potential employees to financial and criminal background checks. Red flags include criminal activity and a history of substance abuse. As in the gaming industry, pharmaceutical security managers indicated that the economic downturn has made bankruptcy or financial hardship so commonplace that it is no longer a useful red flag.

The pharmaceutical industry maintains a "disbanded list" of individuals banned from working with controlled substances, listing individuals fired from producers or distributors under suspicion, people who had been convicted of possession or distribution of illegal drugs, and the like.

Ex-employees are immediately denied access to facilities and their IT systems, no matter the reason for their departure. It is unlikely that an individual terminated for illicit activities would be hired by another pharmaceutical company, and the worst offenders would be placed on the national disbarred list to prevent them from falsifying employment records to conceal their past misdeeds.

Training and Motivating Staff

Pharmaceutical companies give new employees site-specific security training as well as training required for HIPAA and other regulatory compliance. At pharmaceutical production sites, individuals selected to work with controlled substances are required to undergo additional training.

HIPAA requires annual refresher training, and most corporations conduct annual or quarterly security training as well. DEA and FDA audits and short-notice inspections help ensure that site managers and employees remain vigilant.

One interviewee in particular emphasized that security vigilance is a by-product of a security-conscious corporate culture that recognizes theft prevention as an essential element of brand protection and operational success.

Controlling, Monitoring, and Accounting for the Items to be Protected

When API is received at a production facility, workers measure its weight, and then subject it to a number of quality checks to ensure purity before clearing it for production. The two-person rule is in effect when workers open an API vault, remove a specific amount (by weight), secure the vault, and transport the API to the production line, where they confirm its weight and purity once more.

The production line is under constant camera surveillance, as are the inside and the outside of the vaults. The CST and security personnel also monitor the production lines. The factory produces pills in batches of modest size, making it possible for the accounting system to measure input and output, and localize any identified losses, more precisely than would be plausible in a continuous process.

QA tests pills from every production lot. If QA finds that the percentage of API is low in randomly selected pills, they would first suspect and investigate the possibility of misformulation or inadequate mixing. If the reason for the low API percentage cannot be determined, then security is notified to investigate the possibility of API diversion. If a machine jams and pills fall onto the floor, the line is halted and each pill is retrieved, accounted for, and destroyed.

The vast majority of pills are packaged in large-capacity bottles (commonly 100-pill for brand-name, 1,000-pill for generic controlled substances) and shipped to a wholesaler. A small

percentage of the pills destined for in-patient facilities are packaged in blister packs. Both types of packaging include "tamper-evident" seals. (Tests have suggested that thieves may be able to defeat many types of seals, however.[14])

Once the wholesaler takes custody of the FDF, the responsibility for its security transfers from the manufacturer to the distributor. The wholesaler typically ships the product via regional distribution centers, and then on to pharmacies. Pills are repackaged into the appropriate pill-count bottle after each prescription is verified. Distribution site QA randomly samples filled prescriptions to ensure that they include the correct number of pills.

One pharmaceutical distribution site security manager explained that bottles of pills are purchased by weight, not pill count. To ensure that they never fall below their contractually required weight, it is not uncommon for manufacturers (particularly of generic pharmaceuticals, including generic narcotics) to overfill bottles, including 1,005 pills or so in a 1,000-pill bottle. If a prescription bottle comes up short, this "gain" is used to offset it at no additional cost. One interviewee acknowledged that such errors "did happen," given "the [tens of thousands] of prescriptions we filled each day."

Limiting and Monitoring Insider-Item Interactions

Vaults for controlled substances and their active ingredients are under constant camera surveillance. Only specified personnel can access the vaults, and only with two people acting together. The workers measure the material both when it leaves the vault and when it arrives in the production area. The production area is under surveillance by security cameras and watched by security and by the CST.

At distribution sites, some prescriptions are filled by machine; licensed pharmacists and pharmacy technicians fill the remainder by hand. A limited number of individuals handle controlled substances, and security cameras are trained on them to detect any attempt to divert critical pharmaceutical materials. Like the casino industry, both pharmaceutical producers and distributors require pocketless uniforms to discourage casual theft.

Conducting Investigations

Here, too, interviewees did not provide substantial detail on how their companies conduct investigations when they suspect employees of theft. As with casinos, evidence from surveillance cameras plays a major role in raising initial suspicions and providing evidence. Overall, it does not appear that investigations themselves are a major element of the insider protections at pharmaceutical facilities.

Assessment, Testing, and Learning

Pharmaceutical security managers reported conducting red-team exercises in which participants brainstorm diversion scenarios and security personnel simulate countering them. These exercises help identify potential vulnerabilities and stimulate vigilance.

Learning from and sharing experience are also critical elements of pharmaceutical security programs. The Pharmaceutical Security Institute (PSI) maintains a database of pharmaceutical-related incidents. Data are collected on a voluntary basis, but, according to multiple interviewees, the database is comprehensive. A security manager contacts the PSI to report an incident; if the PSI has similar incidents in their database, they will put the security managers from both victim-companies in touch with each other. Contact is voluntary, but security managers report enthusiastically following through to learn from each other's experiences. (Since brand protection is a key goal, PSI covers both counterfeiting and thefts of controlled substances, with its main emphasis on counterfeiting. In the case of thefts, the incident database focuses on very large incidents, valued at $100,000 or more.[15])

In addition to the PSI database, one manufacturing firm reported a more informal supply-chain security database focusing on cargo theft, maintained by their security staff. Now collecting data from multiple companies as well as state and local law enforcement officials, this unofficial consortium provides a "safe space" for security professionals to discuss challenges they face, exchange data, and discuss legislation that impacts their efforts.

Potential Weak Points

The pharmaceutical security system also has potential weaknesses. Resourceful thieves could defeat the seals on bottles and blister packs to remove pills without detection. The extra pills packaged to ensure compliance with contracted weight requirements appear ripe for diversion. No standard exists for the number of "extra" pills per bottle, and pharmaceutical distribution sites consider this gain a windfall rather than an accounting concern.

The pharmaceutical industry may also be in danger of falling victim to the halo effect. Every interviewee emphasized that their employees were licensed professionals, held accountable to the APA code of ethics—yet it is not obvious that this substantially reduces the risk that these individuals will participate in insider theft. Doctors and nurses who steal medications face similar professional penalties, yet such theft remains an ongoing problem. There is a danger that this belief in the honesty of licensed professionals may lull security professionals into overlooking suspicious acts.

There is also the possibility of surreptitious theft while insiders are handling the drugs. Casino dealers manage to palm chips despite sleeveless uniforms and multiple security cameras; pharmaceutical workers may be able to do the same, with far smaller pills.

Pharmacies themselves represent another potential weak point in the system. Several interviewees argued that theft of Schedule II pharmaceuticals is most likely to occur at individual pharmacies. Burglaries targeting controlled substances are not uncommon, and fraudulent prescriptions are a major concern. Indeed, some pharmacies have given up carrying drugs in particular demand among violent thieves. See Figure 5. The extent to which insiders are involved in these thefts cannot be determined without access to arrest and prosecution records, but cannot be discounted.

Figure 5. Fearing theft, pharmacy no longer stocks controlled substances

Recommendations for the Nuclear Industry

The casino and pharmaceutical industries, of course, are not the same as the nuclear industry. In particular, both can afford to take the attitude that small thefts may not be cost-effective to prevent. Moreover, every facility is unique and must implement insider protections best suited to its particular circumstances and processes.

Nevertheless, this analysis of insider protection in the casino and security industries suggests some approaches to insider protection that the nuclear industry should consider.

Constant video surveillance of both vaults and all insider-material interactions. Both the casino and the pharmaceutical industries use security cameras to monitor critical material inside vaults as well as the vault door. Both use constant video surveillance when insiders are handling critical material. While it may seem redundant to monitor both the vault interior and door, there have been a number of major thefts in other industries that involved people gaining access to the inside of the vault by unorthodox means—such as tunneling in from underneath—and surveillance inside vaults would help deter insiders with legitimate access from palming critical material from the vault. Similarly, constant video surveillance may seem redundant with two-person rule, but provides an additional layer of detection and therefore of deterrence of insider theft.

Frequent and rigorous material accounting. Casinos devote a special vault to counting their cash, and require a rigorous two-person count at the end of every shift. The pharmaceutical industry requires rigorous accounting of input materials and product, in batches small enough that uncertainties could not cover a major theft. Nuclear facilities handling weapons-usable nuclear material in bulk forms also typically require detailed accounting for the material, but opportunities for more frequent and localized accounting may exist that would not substantially increase costs.

Requiring everyone who touches critical material to sign for it. The gaming industry's practice of requiring every individual who touches cash or chips to sign their name and vouch for count accuracy could also be used more widely at nuclear facilities. Though a determined thief will likely be undeterred, this simple and inexpensive process could provide three distinct benefits:

- Increasing security awareness and personal responsibility ("I signed for it, I better make sure it is properly accounted for").
- Providing a record of critical material movement. This "paper trail" could provide an investigative starting point should critical material go missing.
- Offering insight into irregular employee activities (repeatedly forgetting to sign for critical material or falsifying or tampering with the signature card would call for further scrutiny).

Implementing an expanded two-person rule. Both gaming and pharmaceutical security operations expand on the two-person rule by requiring that the two individuals be from different departments. Individuals who report to different chains of command and who do not regularly interact are less likely to form the kind of trust required for successful collusion, or suffer the same disgruntlement to motivate theft. Some nuclear facilities follow similar practices: to open the warhead storage bunkers at the Pantex plant near Amarillo, Texas, requires lifting off a multi-ton block from the door using a specialized forklift, and then opening two locks, the key to one of which is held by the operations staff, the other by security (personal observation, 1995). This simple practice could be incorporated more widely at nuclear facilities.

Rewarding attention to security. One step every organization should take is to consciously reward, rather than marginalize, employees who point out security vulnerabilities and options for improvement.[16] At the very least, an anonymous tip-line should be installed (and its contents acted upon) to remove the fear of reprisal as a barrier to reporting concerns and to convince employees that concerns will be addressed.

Seeking widespread buy-in to the importance of security. A number of pharmaceutical security managers explained that they strive for security buy-in by emphasizing corporate commitment to being a steward of public health, and that good security protects the work and livelihoods of every employee. While buy-in may take years to achieve in full, similar tacks simultaneously appealing to emotion (patriotism, or the desire to prevent a nuclear disaster) and pragmatism (security is here to protect my work) may be fruitful.

Splitting security and surveillance. This practice has both advantages and disadvantages, which may explain why casinos have adopted it and pharmaceutical plants have not. Surveillance teams independent of security could make it more difficult for a security officer and a technician with access to material to collude to steal material. Moreover, surveillance officers are probably better able to monitor the activities of all facility employees objectively, avoiding the halo effect. On the other hand, with only the information available from security cameras and alarm systems, they may not be privy to information about particular people that might help them interpret what they are seeing.

The educated professionals employed at nuclear facilities may resist the Big-Brother-is-watching atmosphere that exists at most casinos. *Security* officers, therefore, should be the trusted and approachable face of security, while the surveillance team remains largely unseen.

Involving regulators in design. One pharmaceutical producer described DEA involvement "at the blue-print stage" of facility design, reviewing approaches and making suggestions. In the nuclear industry as well, it might be worthwhile to involve regulators and security experts from the earliest stages of design, to help achieve a "security by design" approach in which cost-effective security measures are designed in from the outset.

Establishing threat databases and experience sharing. As discussed above, the PSI maintains a database of all pharmaceutical-related crimes. Similarly, the casino industry shares information on crimes and criminals their businesses confront; as one example, commercial firms are in the business of providing software that allows the casinos to easily put photos and names of card counters, thieves, and others excluded from their casinos in a shared database. (There are several such firms; one of the leading companies is Biometrica Systems.[17]) Outside researchers have also developed extensive databases on insider cyber incidents related to critical infrastructure.[8]

Properly administered, similar databases could provide a wide range of benefits to nuclear security operations. Such an effort might include both databases for particular countries administered by national institutions (such as the National Nuclear Security Administration in the United States) and databases serving the broader international community, perhaps administered by an organization such as the World Institute for Nuclear Security.

These databases should include specifics of real cases of nuclear material theft (modus operandi, responsible parties, etc.) and near-misses that did not culminate in the actual loss of material. It would also be worthwhile to include selected incidents at non-nuclear facilities that may help inform nuclear security managers about adversary capabilities and tactics to be protected against.[18] This could include, for example, cases of multiple insiders conspiring together to steal money or other valuable items; cases where outsiders and infiltrated insiders worked together to defeat elaborate security systems such as the remarkable Antwerp Diamond Center heist in 2003[19]); and more.[20] Ideally, the institution managing the database should employ professionals to regularly analyze it for trends, lessons learned, and potential threats.

To maximize effectiveness, the database should not be overclassified, and should be widely available among nuclear security professionals and site managers. If parts of the database required higher classification, they could be separated from the rest.

Potential benefits of national and ultimately international databases of this kind include:

- **Increasing vigilance.** One of the reasons to make such databases widely available to nuclear security managers is to help increase vigilance and threat awareness. The attitude that "it will never happen here" is more easily overcome when one can point to numerous recorded incidents in which it did, or almost did.
- **Connecting the dots on threat information.** Adversaries carrying out surveillance on one facility may be watching other facilities as well—and the nature of the activity may become clear if these facilities are exchanging information. An employee report of being approached by a suspiciously curious stranger might be overlooked at one facility, but might provoke increased scrutiny if observed at multiple facilities.
- **Sharing best practices, jointly developing solutions.** The PSI database of pharmaceutical crimes encourages security

managers who have experienced similar incidents to contact each other. Interviewees indicated that the additional transportation security database discussed earlier also provides a forum for discussion of real incidents and potential responses.

- **Improving responsiveness to emerging issues.** Data might include premature failures or unexpected weaknesses in security technologies, issues with new procedures, and the like. With these data from other facilities in hand, security managers would be better able to foresee vulnerabilities and allocate budgets, allowing security to move from reactive response to incidents to proactive anticipation of vulnerabilities.
- **Strengthening employee buy-in.** Individual facilities might encourage employees to review information from the database and help prepare their own site's data for contribution, helping them to understand the reality of the threat and to be on the lookout for relevant information.

In the world of nuclear safety, sharing of operating experience, including incidents that could have a safety implication (such as clogged pumps or cracked equipment) has been an absolutely central element of the dramatic increase in nuclear safety achieved in the decades since Three Mile Island. In the United States, each reactor is a member of the Institute for Nuclear Power Operations (INPO, the U.S. arm of the World Association of Nuclear Operators, or WANO), and is required to provide reports on each safety-related incident, with an analysis of root causes and lessons learned. INPO analyzes these reports, and distributes lessons learned bulletins to all operating U.S. reactors. Moreover, INPO reviews and rates each facility's implementation of these lessons learned.[21] No comparable process exists in nuclear security, either at the national or the international level.

The use of some or all of these practices from the casino and pharmaceutical industries may help the nuclear industry reduce the risks of insider theft. But there is no magic bullet. Insiders, with their authorized access to facilities and knowledge of the facility security system (and, potentially, its vulnerabilities) will remain a significant challenge for nuclear security. Finding ways to keep employees motivated and loyal, to build strong security cultures with widespread employee buy-in to the need for stringent security, and to give employees incentives to identify and resolve potential vulnerabilities, will remain difficult management problems. Difficult challenges also arise in striking an appropriate balance between respecting employees and remaining aware of the danger that any insider could commit criminal acts. Constant vigilance and an approach focused on continual adaptation and improvement will remain necessary.

Acknowledgements

The authors would like to thank the pharmaceutical and casino security managers who gave us their time, insights, and access to their facilities; they prefer to remain anonymous. We are grateful to the Global Nuclear Future Initiative of the American Academy of Arts and Sciences, which provided funding for this research. Our thinking was clarified and strengthened by comments from participants in a workshop on insider threats sponsored by the American Academy, held at Stanford University in December 2011. We are also grateful to the Belfer Center for Science and International Affairs at the Harvard Kennedy School, which provided travel support for interviews, and to the Nuclear Threat Initiative, which supported the research that helped us develop the overall framework described here.

Matthew Bunn, an associate professor at the Harvard Kennedy School, is a former advisor in the White House Office of Science and Technology Policy and the author of the Securing the Bomb *series of reports. He holds a Ph.D. in Technology, Management, and Policy from MIT.*

Kathryn M. Glynn, a consultant for the Department of Defense in IBM's Global Business Services practice, is a former naval aviator. She holds a Master's in Public Policy degree from the Harvard Kennedy School.

Endnotes

1. 2010. Communiqué of the Washington Nuclear Security Summit. Washington D.C.: The White House, Office of the Press Secretary. April 13.
2. 2012. Seoul Communiqué: 2012 Seoul Nuclear Security Summit. Seoul: Ministry of Foreign Affairs, Republic of Korea. March 27.
3. International Atomic Energy Agency. 2011. *Nuclear Security Recommendations on Physical Protection of Nuclear Material and Nuclear Facilities*, INFCIRC/225/Rev.5. Vienna: IAEA; http://www-pub.iaea.org/MTCD/publications/PDF/Pub1481_web.pdf.
4. International Atomic Energy Agency. 2008. *Preventive and Protective Measures Against Insider Threats*. International Atomic Energy Agency, Vienna: IAEA. World Institute for Nuclear Security. 2010. *Managing Internal Threats: A WINS International Best Practice Guide for Your Organization*. World Institute for Nuclear Security, Vienna: WINS.
5. This article draws heavily on Glynn, K. M. 2011. *Preventing Insider Theft: A Cross-Industrial Analysis*. (Master's thesis.) Cambridge, Mass.: Harvard Kennedy School.
6. See, for example, Boss, D.J. and A.W. Zajic. 2010. *Casino Security and Gaming Surveillance.* Boca Raton, Florida: Auerbach. Koh, R., E.W. Schuster, I. Chackrabarti, and A. Bellman. 2003; *Securing the Pharmaceutical Supply Chain.* Cambridge, Mass.: Massachusetts Institute of Technology; http://forum.autoidlabs.org/uploads/media/MIT-AUTOID-WH021.pdf; and Pharmaceutical Security Initiative. 2012; http://www.psi-inc.org/index.cfm.

7. For similar definitions applied to safety, see Reason, J. 1997. *Managing the Risks of Organizational Accidents*. Aldershot, U.K.: Ashgate.
8. Keeney, M., D. Capelli, E. Kowalksi, A. Moore, T. Shimeall, and S. Rogers. 2005. *Insider Threat Study: Computer System Sabotage in Critical Infrastructure Sectors.* Pittsburgh, Penn.: U.S. Secret Service and Software Engineering Institute, Carnegie Mellon University.
9. Duggan, R. 2011. Addressing the Insider Threat—A Call to INMM Community Action, *Proceedings of the 52nd Annual Meeting of the Institute for Nuclear Materials Management, Desert Springs, Calif., July 17-21, 2011*.
10. Personal communication with former Russian nuclear weapon designer, 2001.
11. Beam, C. 2010. Ocean's One: What's the Point of Stealing Casino Chips? *Slate.* December 17.
12. See, e.g., 1996. Frontline: Loose Nukes: Interview with Leonid Smirnov. Public Broadcasting System; http://www.pbs.org/wgbh/pages/frontline/shows/nukes/interviews/smirnov.html.
13. Nisbett, R.E. and T.D. Wilson. 1977. The Halo Effect: Evidence for Unconscious Alteration of Judgments. *Journal of Personality and Social Psychology* 35**,** 250-256.
14. Johnton, R.G. 2006. Tamper-Indicating Seals. *American Scientist* 94(6) (November-December), 515-523.
15. Pharmaceutical Security Initiative. No date. The Counterfeit Situation; http://www.psi-inc.org/counterfeitSituation.cfm.
16. Bunn, M. 2005. Incentives for Nuclear Security. In *Proceedings of the 46th Annual Meeting of the Institute for Nuclear Materials Management, Phoenix, Ariz., July 10-14, 2005*. Northbrook, Ill.: INMM.
17. Biometrica Systems. 2012; http://www.biometrica.com/index.html.
18. Hoffman, B., C. Meyer, B. Schwarz and J. Duncan. 1990. Insider Crime: The Threat to Nuclear Facilities and Programs. Santa Monica, Calif.: RAND.
19. Selby, S.A. and G. Campbell. 2010. *Flawless: Inside the Largest Diamond Heist in History*. New York: Union Square Press.
20. See Bunn, M. 2010. Securing the Bomb 2010: Securing all Nuclear Materials in Four Years. Bunn, M., Cambridge, Mass.: Project on Managing the Atom, Harvard University, and Nuclear Threat Initiative; http://www.nti.org/securingthebomb, 95.
21. Rees, J.V. 1996. *Hostages of Each Other: The Transformation of Nuclear Safety Since Three Mile Island*. Chicago: University of Chicago.