ORIGINAL RESEARCH

Agent of Opportunity Risk Mitigation: People, Engineering, and Security Efficacy

Margaret E. Graham, MBA, MPH; Michael G. Tunik, MD; Brenna M. Farmer, MD; Carly Bendzans; Aileen M. McCrillis, MSLIS; Lewis S. Nelson, MD; Ian Portelli, PhDc, MSc, CRA; Silas Smith, MD; Judith D. Goldberg, ScD; Meng Zhang, MS; Sheldon D. Rosenberg, MA, MS; Lewis R. Goldfrank, MD

ABSTRACT

Background: Agents of opportunity (AO) are potentially harmful biological, chemical, radiological, and pharmaceutical substances commonly used for health care delivery and research. AOs are present in all academic medical centers (AMC), creating vulnerability in the health care sector; AO attributes and dissemination methods likely predict risk; and AMCs are inadequately secured against a purposeful AO dissemination, with limited budgets and competing priorities. We explored health care workers' perceptions of AMC security and the impact of those perceptions on AO risk.

Methods: Qualitative methods (survey, interviews, and workshops) were used to collect opinions from staff working in a medical school and 4 AMC-affiliated hospitals concerning AOs and the risk to hospital infrastructure associated with their uncontrolled presence. Secondary to this goal, staff perception concerning security, or opinions about security behaviors of others, were extracted, analyzed, and grouped into themes.

Results: We provide a framework for depicting the interaction of staff behavior and access control engineering, including the tendency of staff to "defeat" inconvenient access controls. In addition, 8 security themes emerged: staff security behavior is a significant source of AO risk; the wide range of opinions about "open" front-door policies among AMC staff illustrates a disparity of perceptions about the need for security; interviewees expressed profound skepticism concerning the effectiveness of front-door access controls; an AO risk assessment requires reconsideration of the security levels historically assigned to areas such as the loading dock and central distribution sites, where many AOs are delivered and may remain unattended for substantial periods of time; researchers' view of AMC security is influenced by the ongoing debate within the scientific community about the wisdom of engaging in bioterrorism research; there was no agreement about which areas of the AMC should be subject to stronger access controls; security personnel play dual roles of security and customer service, creating the negative perception that neither role is done well; and budget was described as an important factor in explaining the state of security controls.

Conclusions: We determined that AMCs seeking to reduce AO risk should assess their institutionally unique AO risks, understand staff security perceptions, and install access controls that are responsive to the staff's tendency to defeat them. The development of AO attribute fact sheets is desirable for AO risk assessment; new funding and administrative or legislative tools to improve AMC security are required; and security practices and methods that are convenient and effective should be engineered.

(*Disaster Med Public Health Preparedness.* 2010;4:291-299)

Key Words: academic medical centers, hazardous substances, security, risk assessment, risk perceptions

Academic medical centers (AMC) are critical to our national ability to respond to a terrorist or other large-scale event, given their role as providers of the health care workforce in an emergency.[1] AMCs also engage in teaching, training, and scientific investigation, and serve as data and biological repositories. AMCs have not routinely assessed their exposure to a misappropriation and large-scale release of potentially harmful chemical, biological, radiological (CBR), and pharmaceutical substances that are commonly used for health care delivery and research. The threat of such substances, defined as agents of opportunity (AO), is not well understood, as opposed to the known and recognized harmful health effects of select agents and toxins,[2] chemicals of interest,[3] controlled pharmaceuticals,[4] and radionuclides of concern[5] ("select agents"). A less-stringent regulatory environment creates a potential for AOs to be used maliciously when a complementary dissemination mechanism is available, thereby creating an unrecognized risk for a disaster within the institution. This AO risk exists when 3 components are present: threat (presence of a high risk agent), vulnerability (accessibility to the agent and its means of dissemination), and consequence (compromised facility operations or harm to human health). AMCs can increase their

©2010 American Medical Association. All rights reserved.

https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

resiliency by reducing or limiting their AO risk. Although beyond the scope of the present AO study, it is expected that such measures would also protect building structures that share AMC dissemination characteristics, including office complexes, shopping malls, and sports/entertainment arenas with uncontrolled public access.

The AO study identified potential AOs within a single medical school and 4 AMC-affiliated hospitals (the AMCs) and assessed the vulnerability of the AMCs to AO disasters and the resultant consequences. This was accomplished through a survey that assessed health care workers' knowledge of AOs, interviews that gathered facility-specific information concerning AOs, and workshops that determined the AMCs' organizational reaction to AO threat scenarios. These activities produced a list of AOs found commonly in urban AMCs, an AO profile detailing information important to a response to specific AO events, and a framework for understanding the dimensions of AO risk and the subsequent likely AMC response.[6]

Overall, strong security controls were found to play an important role in the efforts of AMCs to reduce or eliminate their AO risks. A key determinant of security efficacy is the degree to which staff accepts or rejects the need for a particular set of access controls such as locked doors and card swipe systems. Employee perceptions of inconvenience are a major influence on their behaviors, leading employees to devise strategies to "defeat" access controls intended to secure locations within a particular building.

This article addresses the principles of human factors engineering, which incorporates human abilities, expectations, and limitations into work environments, systems development, and device design.[7] Such thinking is incorporated into clinical care through patient safety strategies, but it has not yet been extended to AMC infrastructure security. We developed a 2-way model of combined hospital/research security efficacy, suggesting that the presence of an access control is insufficient to denote a secure location, although such an indicator is used commonly as a performance measure. It illustrates that the effectiveness of a given access control (engineering) is limited by the degree to which the staff believes that the inconvenience created by the control is necessary (people/behavior) and calls for further research into this question. Such a framework is compatible with the all-hazards approach and the disaster management training and education competency recommendations promulgated by disaster medicine experts.[8]

METHODS

After obtaining commitment of support from AMC leadership, e-mails were sent to the Environment of Care Committee membership at the 4 hospitals and the departmental administrators at the New York University School of Medicine, explaining the study and asking them to nominate themselves and suggest other people as sources of information concerning AOs. This process created the potential participant pool, consisting of a representative cross-section of operations and academic disciplines and departments. Through exploratory, inquiry-generating open-ended interviews with selected pool participants, representing all levels of authority, institution-specific data concerning agents and dissemination mechanisms were collected from the participants about the AMCs.

The interviews were originally structured to accomplish a single objective: the gathering of logistical facts about potential AOs. Interviews were conducted in the location chosen by the interviewee (offices and conference rooms). Written notes were taken with the permission of the interviewee during the session and were transcribed by the interviewer.

The interviews followed a prespecified format: the investigator reviewed the human subject rights and protections accorded by the study project summary statement (including confidentiality), presented an overview of the study, obtained the interviewee's informed consent for participation, and then asked a series of general questions to ascertain the interviewee's current title, length of employment in that title, and the respective department's organizational chart. This information was used to code interviewees by location, department or discipline, and title. The human subject protections complied with the requirements set by the Department of Veterans Affairs (VA) institutional review board, the institutional review board of record.

Interviews gathered data about the locations of CBR and pharmaceutical agents (agent acquisition sites) and (2) air-handling units, kitchens, cafeterias, and water tanks (agent dissemination sites). If the interviewee worked in or had knowledge of an agent acquisition site, then the questions were designed to identify available agents (eg, How much of the agent is usually on hand in your location? How does it arrive? Where it is kept and how it is used? Do you think this agent can cause harm to large groups of people? Is there a psychological component to this potential exposure?). Agent acquisition sites included diagnostic and therapeutic clinical departments, clinical and research laboratories, cleaning material and other supply sites, loading docks, waste disposal, and pharmacies.

If the interviewee worked in or had knowledge of an agent dissemination site, then the questions focused on understanding how the dissemination mechanism functioned and the scale and scope of that mechanism's footprint on a particular building or combination of buildings (eg, Where is the mechanism located? How many such locations exist? What is the metric that characterizes this mechanism: cubic feet per minute for air-handling units, gallons for water, meals for food services, etc? What segment(s) of the building are supplied by this location?). Agent dissemination sites included mechanical and engineering rooms and spaces containing air-handling units and water tanks, elevators, kitchens and cafeterias, and central supply.

A series of questions was asked to determine whether an unauthorized individual could plausibly enter the agent acquisition site, obtain a quantity of the agent, and remove it for use elsewhere. The same line of questioning was used with staff working in the agent dissemination sites to learn whether an unauthorized individual could enter that area, gain access to the dissemination location, and leave the area undetected. On-site inspections of the agent ac-

©2010 American Medical Association. All rights reserved.
https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

quisition and dissemination sites were made, accompanied by an AMC or affiliated hospital interviewee. Inquiries with regard to the security practices at the access controls (locked doors, cameras, swipe or pass card interlocks, video cameras, and security patrols) were made at the time of the visual inspections. This information was used to generate the threat scenarios that were later presented for discussion and analysis to the member institutions of the AMC.[6]

Once the primary objective of gathering AO information had been met, additional questions were presented during interviews: (1) "Hospitals should be 'open environments.' Everyone should feel welcome to walk through the front door. Do you agree or disagree? Please describe why." (open environment question) and (2) "If you had control of $100,000 and a charge to improve security either in your area or in another part of your institution, where would you spend it?" (security improvements question). A definition of "open environment" was not provided. Comments concerning security were extracted by the coprincipal investigator from the transcribed notes and incorporated in a structured database (Microsoft Excel 2007, Microsoft Corp, Redmond, WA). Themes emerged based on the concepts identified within those comments, without regard to how many times a particular location, department or discipline, or even a particular interviewee, was cited.

To identify published literature relevant to AMC security, several search methodologies were used, including a structured literature search in the major biomedical databases, a review of the gray literature, and a hand-search, and following the recommendations of local experts and colleagues. The biomedical databases MEDLINE, Embase, HealthStar, PsychINFO, Web of Science, and Google Scholar were searched using the different variations and combinations of the following search terms: *universities, academic medical centers, medical schools, hospitals, health facilities, hazardous substances, agents (biological, chemical, pharmaceutical, radiological), dual-use research, security, risk management, risk analysis, risk perception, public opinion, attitude, biosecurity, biosafety, access control, bioterrorism, terrorism, disaster, preparedness, warfare, weapons, mass casualties, food contamination, air pollution,* and *water pollution*. The search was limited to articles written in English. A gray literature search was less structured but focused on US government and regulatory agency documents, policy institute publications, and news media.

RESULTS AND COMMENT

Eight themes emerged from a review of the security-related comments extracted from the interviews conducted (N = 147) across the AMCs. Twenty-nine specific comments illustrating the themes in question were extracted from 25 of the 147 interviews. These 25 interviews involved administrators (3), faculty (6), clinicians (1), directors of departments (7), supervisors (5), and front-line workers (3). These interviews were distributed across departments and disciplines as follows: administration, including directors (8), academic programs, including researchers and faculty (4), registered nurses (1), facilities management (1), clinical laboratory (3), materials management (3), and security and safety staff (5). In 4 instances, 2 comments supporting different themes were drawn from the same interview; 1 involved an administrator and the other 3 involved security/safety staff.

AMCs are complex organizations combining multiple missions, patient care, research, and teaching.[9] These organizations prefer to present a welcoming "open front door" to large numbers of people entering their premises in the normal course of a day, maintaining that atmosphere throughout patient units and public spaces such as the main lobby and cafeterias.[10] At the same time, security must control access to certain locations either because of patient safety concerns (eg, psychiatric, newborn, and pediatrics wards) or because they contain materials used in health care that are recognized as capable of causing harm to people and/or the environment if not controlled, such as laboratories designated as Level 3 or 4 under present biosafety standards[11] or locations containing certain radiological substances or devices.[5] Finally, security plans must conform and adapt to the research mission, which combines elements of both open and controlled environments.

Although information concerning security, employee behavior, and employee perceptions appears to be central to AMCs seeking to effect change in their security practices, prior work by security professionals in this area is limited.[12] Hazard vulnerability analysis and other types of risk assessments in health care settings commonly consist of completing a checklist, noting the access controls that are in place for sensitive areas, identifying deficiencies (eg, broken cameras, locks that need to be replaced), and devising a plan to manage the deficiencies.[13] The VA hospital system employs armed police and security and inventory controls over selected CBR agents owned by or controlled at VA facilities, far stricter than nongovernmental hospital standards. Nevertheless, a 2006 Office of the Inspector General report found certain VA hospitals to be noncompliant with regard to employee training and security access protocols.[14] Security professionals are well aware of the need for employee support and involvement with security[15]; however, information concerning employee security practices is not required by any of the accreditation standards, codes, or regulations (personal communication, Healthcare Facility Security Workgroup of the Joint Advisory Work Group, Healthcare and Public Health, Critical Infrastructure, and Key Resources Sector, August 31, 2009).

Evidence of the influence of human factors is found in publicly reported assessments of university compliance with select agent regulations. Even under circumstances in which the agent threat is well documented, facilities failed to comply with clearly defined standards and were cited for infractions such as lapses in access procedures as required by their own security plans.[16] A recent critique of the safety practices of select agent research sites in academic institutions and high-tech private company facilities found evidence of a research laboratory culture that disregards worker and public safety and called for trans-

©2010 American Medical Association. All rights reserved.

https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

formation through the development of safety culture concepts and practices.[17]

The AO interviews provided insights into the range of staff perceptions of AMC security strategies. Comments that recount interviewees' statements are denoted by quotes; otherwise, the comment is paraphrased (PF). The concepts that have implications for reducing or eliminating AO risk are listed as themes.

Theme 1: Staff Security Behavior Is a Significant Source of AO Risk

Interviewees described a range of staff security behaviors, including the degree to which staff propped open doors that should be closed and locked, a behavior usually attributed to the frequency of ingress or egress, which made opening and locking the doors highly inconvenient; defeated identification card swipes by politely holding the door for other people ("piggybacking"); and avoided stopping and questioning unknown individuals in their work area. These "weak" behavior patterns represent an important cause of the vulnerability of agent acquisition and dissemination sites.

> (PF) Security is deficient. There have been a number of computer thefts. Our major security issue is stolen property, usually things that are portable and "fence-able."

> "Anyone dressed as (an) EMT could walk around with no one questioning them. Anyone with a white coat can walk just about anywhere."

> "The biggest problem is keeping fire doors closed—employees like to prop them open."

> (PF) Security is inconsistent. Sometimes people are permitted to enter, and protocols are not followed uniformly.

The same behaviors have been observed even in the presence of highly toxic select agents. A 2004 Office of the Inspector General inspection at 11 university-sited high-security select agent research laboratories ("hot labs") found the following[18]:

> All of the universities had weaknesses in preventing unauthorized entry into "hot labs" and unauthorized removal of select agents. Intruders could have accessed buildings housing hot laboratories by entering through unlocked doors and hallways, "piggybacking" (following closely behind authorized persons), bypassing security officers, or forcing access through unalarmed doors. Further, at all 11 universities, once inside the buildings, intruders had unobstructed access to the floors with hot laboratories.

The manner in which staff "defeated" security access controls was routinely described, demonstrating a pervasive lack of acceptance of such controls. Security professionals suggest that it is important to change people's behaviors, but that education and training alone are insufficient.

> "I think of safety for my patients all the time, but rarely about my safety or that of my employees. We are all very busy . . . we tend not to pay attention to people and things around us."

The staff perception that security is "someone else's job" is an obstacle to effecting a change in behavior.

> "The problem is that most people do not want to be involved in security. They don't want to be the ones challenging or enforcing any rules."

> (PF) Security is not singularly and exclusively a security guard issue, that the whole community needs to be involved . . . I recommend a campaign similar to that of New York City's "see something, say something" initiative for the health care community. "Propped doors" are a case in point. There is no other way to stop people from propping doors open.

Applying the concept that human behaviors influence the effectiveness of access controls, the Figure depicts a 2-way table cross-classifying the alterations in strength of access controls by different levels of security practices. The horizontal (X) axis (abscissa) of the figure demonstrates the alteration in strength of access controls (engineering), the interventions that use mechanical/electrical devices, or the presence of a security guard to limit access to a location. The point of origin is a completely open location where anyone can enter, no cameras are present, and individuals can move freely without detection. Such locations are considered to have weak access controls. Movement along the abscissa indicates the presence of ever-sturdier locks, more sophisticated closed-circuit television cameras, and/or regular security patrols, eventually denoting strong access controls, which include motion detectors, 24-hour guard posts, and alarmed doors that trigger an immediate security lockdown.

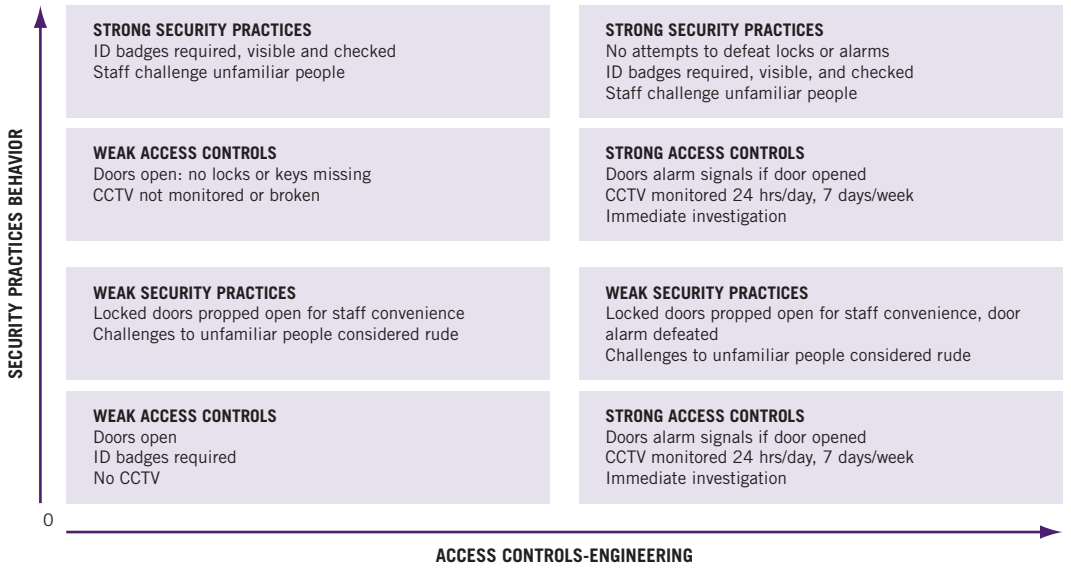
Security practices (behavior), indicated along the vertical (y) axis (ordinate) of Figure 1, are the individual and group behaviors of staff working in a given location. Weak security practices at the origin are demonstrated when nonsecurity staff express little or no respect for access controls, circumventing them through practices that render the control(s) ineffective. These practices include a reluctance to challenge the presence of unfamiliar personnel in an area, regularly propping open doors, and letting others gain admittance to an area without challenge. Strong security practices are exhibited when staff routinely challenge anyone who is unfamiliar to them, insist that anyone requesting access to an area follow appropriate protocols, and routinely secure the locks on doors in rooms and cabinets in their work areas.

Application of the strong/weak combinations of access controls and security practices support the conclusion that anything less than strong in both dimensions renders an agent acquisition and/or agent dissemination site vulnerable to AO risk. Therefore, access controls alone are imperfect mitiga-

©2010 American Medical Association. All rights reserved.
https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

FIGURE

2-way table cross-classifying the alterations in strength of access controls by different levels of security practices.



tion strategies for reducing or eliminating AO risk in AMCs. Either staff behavior must be changed or the nature of access controls need to be revised. Ideally, the impact of access controls must be small, presenting minimal inconvenience to staff.

Controls characterized as effective were found in some areas subject to little foot traffic:

> "One must go through a door with both a key and card swipe on the xxth floor to gain access to maintenance rooms. The doors leading to the maintenance rooms on and above floor xx are alarmed when left open for a certain amount of time." [the identity of floor numbers was changed]

Strong practices and weak access controls depend on a strong security climate.

> (PF) Additional security is not necessary. **Any stranger entering the area will be stopped and questioned**, that staffing in the laboratories is sufficient now. [emphasis added]

It is important to note that other people working in the same area did not agree with the latter person's assessment and thought that owing to the volume of people entering this location throughout the course of a day, strangers would not be challenged.

Efforts to move the security practices of an AMC staff from "weak" to "strong" require an understanding of the factors that influence individual and group behavior. The influence of emotion and individual judgments and the fact that risk means different things to different people are major factors to be considered.[19] Concern about unintentional occupational exposures prompted a self-assessment by select agent researchers, which included recommendations that emphasized the importance of engineering controls, training, and an active biosafety program.[20] A study of homeland security strategies[21] found that people rate security practices as positive, desirable, or effective when they are not personally intrusive, such as those for an airport passenger or baggage screening. People rate security practices as ineffective when they are personally intrusive such as personal location tracking by cell phone.

> (PF) Security is not an issue. I feel pretty comfortable here. I have worked in a reference lab where security levels were much higher: a mandatory bioprint access control system required each staff member to constantly "put their finger on a pad," which I found to be inconvenient, "a little much."

Given the importance of people's acceptance of inconvenience in establishing the effectiveness of access controls, attention should turn to examining the sources of AO risk, the AOs themselves, and their dissemination mechanisms. Other work done in the AO study provided the data needed to model and simulate the dissemination of an AO, which provides an opportunity to examine new engineering interventions that may replace the need for inconvenient access controls. Technology was identified as the greatest need by safety and security

©2010 American Medical Association. All rights reserved.
https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

professionals participating in a 2007 survey involving 656 hospitals conducted by GE Security and the International Association for Security and Safety.[22]

Theme 2: The Wide Range of Opinions About Open Front-Door Policies Among AMC Staff Illustrates a Disparity in Perceptions About the Need for Security

Responses to the open environment question were reviewed for indications of agreement or disagreement with open front-door practices. Because the interviewees were free to interpret the meaning of the term *open environment* in whichever manner they chose, the stated expression of agreement or disagreement was less important than the explanation provided as justification.

Some individuals agreed that hospitals should be open environments.

> "People should be given the feeling that we are here to help them. When they are here, they should be treated professionally and with as much warmth as we can provide. If we have proper plans in place, we should not have to be overly restrictive."

Those who disagreed usually referred to the entire facility, arguing that there needed to be some type of access control in discrete locations:

> (PF) An institution can be open, yet be secure in key areas. Things can be locked up. For example, no one should be able to access an area that contains radioactive materials. Such agents should be kept in secured areas that are accessible only to specified people.

> (PF) Hospitals need to have an open environment. But they are not like every other public place—there is great potential for harm.

Occasionally, individuals expressed negative opinions about open environments without qualification:

> (PF) Hospitals and schools are not, by definition, open environments. There is an obligation to protect patients and staff members. Not everyone is entitled to enter a hospital.

A typical response to the question indicates a degree of conflict on a theoretical level, where 1 interviewee agreed with the statement by stating:

> (PF) Academic medical centers must function in an open environment. Academic medical centers have multiple missions, including patient care, education, and research. In general, these function best in an open environment. Creation of barriers and restrictions often has unpredictable "chilling" effects on the performance of these functions.

The same interviewee stated later in the discussion:

> "I agree that some areas of a hospital could have more security than other areas."

This illustration of the variety of opinions among AMC staff occupations and disciplines characterizes the challenge that is faced by an institution seeking to control AO risk.

Theme 3: Interviewees Expressed Profound Skepticism Concerning the Effectiveness of Front-Door Access Controls

The installation of physical barriers, physical separation (standoff distance), thorough screening, and other forms of initial restrictive access controls are inappropriate for the large numbers of people, including staff, patients, visitors, trainees, staff, suppliers, and contractors continuously entering and exiting AMCs. Indicative of this, the front door access controls varied at the 4 hospital main lobbies. Two hospitals used roped posts to guide people entering through a checkpoint at which each person wishing to enter was required to show proof of identity (eg, institutional identification card, driver's license). Two hospitals deploy guards and require all bags to pass through metal detectors. Midway into the AO study performance period, structured security checkpoints were removed at 2 of 4 hospital main entrances, creating an open front door. Entrants can now walk freely into those institutions. Security guards are present and information booths are staffed for individuals who are seeking directions or other types of guidance. No other access control is obvious. The study did not elicit opinions concerning this decision, limiting this discussion to the comments shared in relation to the practices that existed at the time of the interview.

Staff were highly skeptical of the effectiveness of the practice requiring identification at the front door:

> "When stanchions were present, it was a lot easier to check ID, and spot a certain party if you were looking for him/her. However, it looked like cattle being herded and it doesn't do much for security. Anyone could have come through, flashing an ID that was never checked."

> "A person can say, 'Going to the 9th floor,' and go elsewhere."

These comments suggest that ineffective access controls create a cynicism about security interventions that may create unnecessary barriers to security efficacy.

Theme 4: An AO Risk Assessment Will Require Reconsideration of the Security Levels Historically Assigned to Areas Such as the Loading Dock and Central Distribution Areas Such as Central Supply; Many AOs Are Delivered to These Locations and May Remain Unattended for Substantial Periods

> "It is common practice to place hazardous waste accumulation rooms closest to the loading docks of health care institutions. This way, such materials are not 'schlepped' through the building, patients certainly don't need access – you sim-

©2010 American Medical Association. All rights reserved.
https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

ply would not give prime real estate to such functions. Because they are tucked away, there is usually not a lot of security that is designed into these spaces."

(PF) The general consensus is that it is easy for anyone to get into the loading dock area. A security guard was stationed at the top of the entry ramp, but that station has been eliminated.

AO risk is commonly found in areas such as loading docks, which have not traditionally attracted security resources. Efficacious security interventions in such areas must be responsive to staff members who are unaccustomed to controls, multiple department interactions, and allocation of costs associated with the introduction of new interventions.

Theme 5: Researchers' View of AMC Security Is Influenced by the Ongoing Debate Within the Scientific Community About the Wisdom of Engaging in Bioterrorism Research

Critics of national security research programs believe that security threats are exaggerated by federal agencies seeking to expand their influence, resources are needlessly diverted from research into problems such as cancer and heart disease, and security measures create unfavorable consequences such as "erosion of scientific integrity and ethical standards through restrictions of basic civil liberties."[23]

"[A] critical tension exists in the research community between the need for collaboration/open science and the issues raised by "dual purpose" efforts. [I am] sympathetic to the conflict that emerges when scientists react strongly to questions of security and their tendency to feel beleaguered."

The research and clinical communities within AMCs may have different opinions about the need for security measures, requiring the customization of access controls so that security interventions are appropriate for each mission.

Theme 6: There Was No Agreement About Which Areas of the AMC Should Be Subject to Stronger Access Controls

The existing controls are primarily designed to stop patients and visitors from wandering into a particular location (eg, roof doors, mechanical and equipment rooms, kitchens) or to secure items subject to theft.

"There are lots of elderly patients who become disoriented and tend to wander—all the more reason for having security."

In areas that have little or no patient traffic, acceptance of the need for access controls appears to decrease.

(PF) There has never been a theft or incident related to security in my laboratory. I disagree with the idea of access controls to my work area. I am in and out of buildings 10 times per day, I like the idea of the 'city-like' nature of the physical plant, and I feel that any segmentation would have a huge negative impact on collegiality. I simply do not see the need for more security.

(PF) The research side of the house should be very open. The hospital side, though, needs a bit more security.

The tendency of staff to be aware of the security deficits in other departments, without acknowledging the challenges that exist within their own workspace, holds major implications for AMCs seeking to control AO risk, given that AOs exist in a broad spectrum of locations under the control of a variety of departments and occupations.

Theme 7: Security Personnel Play Dual Roles of Security and Customer Service, Which Creates the Negative Perception That Neither Role Is Done Well

"People look at us, degrade us. When they need help, who do they call?"

"[We are] expected to be appropriate in all kinds of situations—pastoral care, social work, public relations, emergency management skills—and balance a welcoming atmosphere with the ability to control/contain situations, asserting preemptive authority when necessary. A real skill, and not fully recognized as such. The institution leadership seems unaware of the complexity of the job as they are now defining it."

"Security guards are comprised of two distinct personalities. Some are very nice; others are incredibly rude. An unpleasant air of 'who are you?'"

Some administrators expressed an awareness of this deficit in mutual respect and struggled to devise ways to overcome it.

"The problem is that a clinician might say—here's a threat, yet Security will say, 'That's not my business, that's doctor business.' We need a partnership between security and clinicians, heightened awareness of the environment. The biggest vulnerability is the barrier between clinicians and security."

"It seems as if the sole function (of security guards) is to provide information—why do we need security to do that? Perhaps as the security force becomes more customer friendly, the community at large needs to be more 'security-friendly.'"

"There is lots of dissatisfaction with the current system. I grant that the Security staff is very stressed. Most do a good job. Some of what they are asked to do is difficult."

The security guard staff, if seen as an underused asset, may be trained and deployed to "partner" with the staff from agent acquisition and dissemination sites to develop efficacious security controls.

©2010 American Medical Association. All rights reserved.
https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

Theme 8: Budget Was Described as an Important Factor in Explaining the State of Security Controls

"The department requested a camera, but they have no budget."

(PF) The funds for implementing new security measures fall under the security budget. This can be difficult to manage with multiple requests across AMCs.

Most agent acquisition and dissemination sites are non-revenue-producing cost centers in an AMC budget. Successful AO risk reduction plans must reexamine the size of the security budget and the expectation that such areas must fund their own security costs, and develop innovative ways to allocate funding to agent acquisition and dissemination sites.

Limitations

Because a representative sample of interviewees by location and department or discipline was not part of the research design (which focused on staff most likely to possess information on AOs), the AO interview comments and themes are illustrative in nature only. In addition, comments were analyzed to identify themes for future research, not to ensure that all points of view would be considered or to understand the proportions of staff who agree or disagree with a particular statement. Furthermore, coders used their judgment when assigning interviews and comments to a particular location; this process was complicated by some locations being owned/operated by a combination of the medical school and 1 of the AMC-affiliated hospitals, and that some staff are categorized by more than 1 discipline or departmental group. These limitations preclude the development of any inferences about perceptions at the job title, work unit, or building level. In addition, an individual's perception of risk, of his or her own behavior, and the behavior of colleagues vary. An interviewee may respond differently in a later interview or under different conditions. For example, if an a personal item had been stolen from an interviewee, his or her comments on security or vulnerability may be different than if no such theft had occurred.

CONCLUSIONS

Because AMCs are important to our nation's defense, they need to mitigate or eliminate their AO risk. The preference of AMCs for a welcoming environment for patients need not be sacrificed, but openness creates a difficult security challenge for AMCs: the need for effective access controls of its agent acquisition and dissemination sites that extend beyond the recognized select agents. This issue has additional implications arising from the fact that AO dissemination is not limited to the AMCs themselves, but can occur in many types of closed building environments including theaters, office complexes, shopping malls, and sports/entertainment arenas. Successfully securing AOs requires the acknowledgment that AO risk exists and that installation of traditional access controls alone will not be sufficient to reduce that risk. Rather, the culture of safety and security that has been created in hospitals to protect patients and staff in certain high-risk patient areas such as psychiatry and newborn wards should be assessed for applicability to AO acquisition and dissemination sites within an all-hazards framework.[8]

AMCs should understand staff perceptions of the need for security in a given work location, installing access controls that are responsive to the staff's human tendency to dislike inconvenience. They may find that access controls appropriate for the workflow of the central supply staff may not be appropriate or successful for clinical laboratory staff; research laboratories may require customized solutions. In addition, AMC leadership must ensure that budget practices will provide funding and must reexamine the role and status accorded to security guards, developing strategies that improve the relationships between security guards and AMC staff of all departments and occupations.

Finally, advances in computer modeling and simulation provide an opportunity to create and test new security technologies that do not rely on acceptance of access controls. Engineering solutions that modify the sources of AO risk (the AOs and their dissemination mechanisms) are also suitable for modeling and simulation.

Author Affiliations: Ms Graham, Ms Bendzans, and Drs Tunik, Nelson, Portelli, Smith, and Goldfrank are with the Department of Emergency Medicine; Ms McCrillis is with the Frederick L. Ehrman Medical Library; and Dr Goldberg and Ms Zhang are with the Division of Biostatistics, Department of Environmental Medicine, New York University School of Medicine. Dr Farmer is with the Division of Emergency Medicine, New York Presbyterian Hospital/Weill-Cornell Medical Center. Mr Rosenberg is with the New York University Langone Medical Center, Organizational Development and Learning.

Correspondence: Address correspondence and reprint requests to Margaret E. Graham, MPH, MBA, NYU School of Medicine, Department of Emergency Medicine, Bellevue Hospital, 27th St and First Ave, New York, NY 10016 (e-mail: lewis.goldfrank@nyumc.org).

Funding for this study was awarded by the Telemedicine and Advanced Technology Research Center, on behalf of the US Army Medical Research and Material Command under contract No. W81XWH0710517.

Received for publication April 14, 2010; accepted September 27, 2010.

Acknowledgments: We thank the staff of the AMCs, the medical school, and the 4 AMC-affiliated hospitals. Their time and expertise, shared with the investigators through the interviews, survey, expert panels and workshops, were invaluable in the development of this work. We also thank Ellen Webb, the initial AO study research coordinator.

Author Disclosures: The authors report no conflicts of interest.

REFERENCES

1. Natarajan N. The healthcare and public health sector overview. *Crit Infrastructure Protect Rep*. 2008;7.1:2-3, 18-19.
2. HHS and USDA select agents and toxins: 7 CFR Part 331, 9 CFR Part 121, and 42 CFR Part 73. http://www.selectagents.gov/Select%20Agents%20and%20Toxins%20List.html. Accessed October 8, 2009.
3. Department of Homeland Security. 6 CFR Part 27 Appendix to Chemical Facility Anti-Terrorism Standards; Final Rule. http://www.dhs.gov/xlibrary/assets/chemsec_appendixa-chemicalofinterestlist.pdf. Accessed March 20, 2010.
4. US Drug Enforcement Administration. Title 21 Food and drugs: chapter 13-drug abuse prevention and control. Controlled Substances Act. http://www.justice.gov/dea/pubs/csa.html. Accessed October 28, 2009.

©2010 American Medical Association. All rights reserved.

https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press

5. Table 1: Radionuclides of concern. http://www.nrc.gov/reading-rm/doc-collections/enforcement/security/2005/ml053130250.pdf. Accessed October 8, 2009.
6. Farmer BM, Nelson LS, Graham ME, et al. Agents of opportunity in academic medical centers: agent identification, agent profile, and institutional risk and preparedness. *Disaster Med Public Health Prep*. 2010;4:318-325.
7. Food and Drug Administration. Medical Devices. http//www.fda.gov/MedicalDevices/DeviceRegulationandGuidance/PostmarketRequirements/HumanFactors/ucm119185.htm. Published May 13, 2009. Accessed October 5, 2010.
8. Subbarao I, Lyznicki JM, Hsu EB, et al. A consensus-based educational framework and competency set for the discipline of disaster medicine and public health preparedness. *Disaster Med Public Health Prep*. 2008;2(1):57-68.
9. Blumenthal D, Ferris TG. Safety in the academic medical center: transforming challenges into ingredients for improvement. *Acad Med*. 2006; 81(9):817-822.
10. Hodgson K. First defense. Using design elements to strengthen security efforts. *Health Facil Manage*. 2003;16(3):16-20, 22, 24-25.
11. Centers for Disease Control and Prevention. Biosafety in Microbiological and Biomedical Laboratories (BMBL), 5th ed. http://www.cdc.gov/od/ohs/biosfty/bmbl5/bmbl5toc.htm. Published April 13, 2009. Accessed March 29, 2010.
12. Gotay A. Establishing security awareness guidelines in a hospital setting. *J Healthc Prot Manage*. 1994;10(2):80-83.
13. Chipley M, Kaminskas M, Lyon W, et al. *Reference Manual to Mitigate Potential Terrorist Attacks Against Buildings*. Washington, DC: Federal Emergency Management Agency; 2003:426.
14. Department of Veterans Affairs, Office of the Inspector General. Emergency preparedness in Veterans Health Administration facilities. Report no. 04-03266-51. http://www4.va.gov/oig/54/reports/VAOIG-04-03266-51.pdf. Published January 6, 2006. Accessed March 26, 2010.
15. Waudby MH. Measuring perception as a component of a security assessment. *J Healthc Prot Manage*. 2004;20(2):8-28.
16. Office of the Inspector General, Department of Health and Human Services. Summary report on universities' compliance with select agent regulations. http://oig.hhs.gov/oas/reports/region4/40502006.pdf. Published June 2006. Accessed September 30, 2010.
17. Baram M. Biotechnological research on the most dangerous pathogens: challenges for risk governance and safety management. *Saf Sci*. 2009; 47:890-898.
18. Office of the Inspector General, Department of Health and Human Services. Summary report on select agent security at universities. http://www.ofr.harvard.edu/homeland_security.php. Published March 2004. Accessed September 30, 2010.
19. Slovic P. Public perception of risk. *J Environ Health*. 1997;59:22-23, 54.
20. Jahrling P, Rodak C, Bray M, Davey RT. Triage and management of accidental laboratory exposures to biosafety level-3 and -4 agents. *Biosecur Bioterror*. 2009;7(2):135-143.
21. Sanquist TF, Mahy H, Morris F. An exploratory risk perception study of attitudes toward homeland security systems. *Risk Anal*. 2008;28(4):1125-1133.
22. Rees K. Securing our hospitals—an executive summary of the GE security & IAHSS healthcare benchmarking study. *J Healthc Prot Manage*. 2008;24(1):113-115.
23. Sidel V, Gould R, Cohen H. Bioterrorism preparedness: cooptation of public health? *Med Glob Surviv*. 2002;7:82-89.

©2010 American Medical Association. All rights reserved.

https://doi.org/10.1001/dmp.2010.38 Published online by Cambridge University Press