



Biosecurity Perspectives

Edwin Taylor

United States Air Force (Retired)

Author's Note

This was a presentation at the CDC 8th National Biosafety Symposium, Atlanta, Georgia, 2004.

I'm going to present security issues from the point-of-view of the terrorist. The difference in risk in safety and risk in security is merely that of malevolent, human intelligence. The same kinds of procedures that mitigate risk and safety mitigate risk and security.

Everything we say in security sounds very easy. It sounds pretty simple: Secure that stuff. Keep it out of the hands of the bad guys. Don't bother us anymore. But, as we get into the nuts and bolts, as we wrestle with the philosophical, the technical, the monetary concerns, we realize it is extremely difficult to do. Living organisms are one of the most difficult things to secure because of the nature of living organisms. Very small amounts become very large amounts. Small amounts that we cannot account for, that we cannot see, can become large amounts once taken out of our control by a thief.

Threat? That's what out there. What might happen? Vulnerabilities are the weaknesses we have against that threat. Risk assessment is basically weighing the probability and consequences of those potential events. Where does threat come from? I would imagine that most people have asked everybody that they can, "What is the threat? What is out there? Who is going to do what? What should I be prepared for?"

How many people in the audience have had a security incident at their facility? Is there anybody here from USAMRID? During the 1980s, two individuals armed with handguns, at different times, entered that facility. Neither one was there for hos-

tile purposes. One was there to visit someone and forgot he had a gun. The other one was there to commit suicide because of some personal problems. The visitor who happened to be carrying a gun did not use his weapon, but the suicidal individual did. So, there are things that happen out there. It may be more likely than we like to think. Intelligence estimates tell us who might be out there and what they might be capable of, but if we look at some of the political consequences of intelligence estimates over the last year, we find that sometimes intelligence is wrong. Intelligence estimates are basically a guess. We hope they are the best guess, but they may not be correct.

Design Basis Threat (DBT) is a planning guideline. For example, if you were worried about a car bomb, your Design Basis Threat would be a vehicular-delivered device. You make a conscious effort to decide how big a device, how close to the building, etc. The reason that you make a decision is that your decision about how close to the building and how big a device might be used directly impacts the mitigation efforts and how much money it costs to defend against that threat. The same would be true if you decide an armed intruder might attack your facility. If you decide to consider an armed intruder, you decide as your Design Basis Threat, "Yes, we are going to protect against an armed intruder." Then the question of the security professional would be, "Okay, armed with what?" There is a difference between somebody being armed with a handgun and somebody being armed with an AK-47. This goes from being a guess or an estimate to a concrete thing. That's what the engineers and professionals use to plan.

Methodology or Gaming Basis Threat is a varia-

tion of that the DBT, and that is where you play a mind game and you say, "If I were attacking my facility, what would I do?" When I'm evaluating a facility and somebody asks me for vulnerabilities, I put on my bad guy hat. If I want to get into the facility, what would I do? If I wanted to damage the facility, what would I do? And once you have an idea of that, you know what things you need to protect against, and you can act accordingly.

Your Targets

What might the bad guys' target? The focus, almost exclusively, in all our meetings and conferences, are the select agents, because the government has written a whole set of rules and regulations on what we must do to comply with, in order to possess, use, and work on select agents. But if I'm the bad guy, and I'm the evil, malevolent human intelligence, I have a lot more areas to target. And if I target something else at your facility, not the organisms themselves, but I can damage your facility, can I not get a positive, from my point of view, result? If I can get a bomb into your facility and blow it up, or blow up the half your facility that doesn't even contain select agents, what happens in the news media? What happens to your funding?

Your Organisms

This is a fairly obvious thing, up to a point. What are we talking about here? The security guys talk about inventories, etc. Where are the organisms located in your facility? If you deal with animals, do you deal with infected animals? Do you have the same security on your infected animals and their carcasses that you have on the stock cultures in your freezer? One of the things I know, as the malevolent, human intelligence, is that sometimes the waste products are much easier to get to than the stock cultures. If I want a sample of what you are working on in your laboratory, can I go five blocks away and plug into a laboratory sewer system and pull out a sample? You should notice now that there is a difference between a security threat in a sewer system and a public health threat in a sewer system. A very small amount of material in a sewer system may not be a public health threat, but it may provide me with what I need as far as a sample of what is in your facility.

Personnel

What if I target your personnel? What if your Senior Investigator wakes up to find me in his bedroom and I hold his wife hostage and tell him to go to the laboratory, come back with a vial or else. I had this discussion with Dr. Peter Jarling, and he actually brought it up to me because he realized, after being named in several of Richard Preston's books, that maybe he had put himself into a visible and vulnerable position. If I'm the malevolent guy, and my point is to attack your organization, your facility, what about your folks? What about when they are away from the facility? The facility itself? How long does your lab operate if I destroy your air handlers? For a big facility, what if I damage your electricity? What if I damage your steam-generation capability? What if those actions, although not directly targeted at the lab itself, cause an overpressure problem and you have an inadvertent release? What you have then is a public relations nightmare. I have achieved my goal.

Information

Most of you are in the business of producing information. That's what science is. It's open information. Without open information, we have no science. I also know that there are a lot of organisms that aren't select agents that grow the same way, that have some of the same characteristics. I know that manipulating plasmids inside *E. coli* allows me the same technology of manipulating plasmids in some other organism, and I know that provided I can get a small sample, that some of those same procedures in the laboratory will, in fact, transfer from a less pathogenic organism to a select agent. I also know, as a terrorist, that there is a huge amount of information in the libraries and reference materials of this and other nations that tells me how to do all these things. I may not have access to the most modern technology, but guess what? The weaponization of anthrax was developed in the United States in the 1960s. Some of that work is classified, but believe it or not, everything about how do it is available to those who know where to look. If I'm a terrorist, I already know that. So, trying to hide that information or information geared towards certain, specific organisms may not be effective.

If I'm a terrorist and I show up at this meeting, I look in the back of that book and there is a list of everybody in attendance. Can't I have a reasonable expectation that for every person listed as a being associated with a university that at that particular university I will find select agents? As a terrorist, my expectation is pretty high. Why else would you be here? That's open information. It's available to anyone who might wish to obtain it, and we don't think about it because we live in a free society where that information exists. What am I telling you? I'm telling you that there are certain things we might want to restrict, like building blueprints and security codes and people's home phone numbers; however, there is other information that trying to put a lid on it is probably impossible. Now, it becomes a question of cost. Do we go through all the trouble to classify information that I can obtain other ways, or do we take that money and put it somewhere else? That is a management decision. As a terrorist, I laugh if you classify your work on *Bacillus anthracis*. I laugh if you classify stuff on how to make it into a powder. If I know the secret of Arid Extra Dry, I know the major secret of weaponization of microorganisms.

Operational Process

As an evil terrorist, my most fruitful target is to directly attack your operation and the operation of others. If I wish to conduct biological terrorism in the United States, what must I attack first? It would be the ability of the United States to deal with such terrorism. Where is the ability of the United States to deal with that terrorism? At all your facilities, your operations, etc. So, if I can do something that shuts down your operations, I remove you as a threat. If I do something to your facility or near your facility that causes people to think there is a problem, and that you have a malfunction, the regulators will shut you down. If my point is to make a terrorist statement, if my point is to shut you down, I can do it and I won't even have done anything overt.

Threats and Vulnerabilities

What might I do? Well, I have three basic ways I'm going to come after you. The first one is an overt attack. I just attack you. The next is clandestine entry attack, and the last one is an operational disruption attack.

Over Attacks

The first is a standoff attack and all that means is I am outside your facility and I shoot someone. For example, you have a laboratory and you have lots of windows. I take a rifle and shoot holes in the windows. That's a standoff attack. Do we have sniper incidents in the United States? If you are located in Fallujah, Iraq a standoff attack is somebody with mortars and rockets. So, some of your vulnerabilities have to deal with where you are. The second is a proximity attack: That is where someone gets close to your facility and does something. A good example here is a car bomb, a vehicular device. Does that happen in the United States?

The last is a penetration attack. This is where I just come through the front door and start shooting, or I drive a vehicle into your building, or I fly an airplane into your roof. Those things happen in the United States. The most common hostile event in the work place is a penetration attack, and that is where the disgruntled individual shows up at the door, either mad at a supervisor or mad at a significant other, is armed, and goes into the facility, or office, or post office, or school, and starts shooting. Statistically, that can happen anywhere. Airplanes have been flown into buildings in the United States.

Clandestine Attacks

This is where a person or persons sneak in and sneak out. This is everything from the intelligence agent, a.k.a. James Bond or Mission Impossible, to the criminal who has decided that you have a lot of nice lab equipment, and he'd like to take it. This includes the outsider, who is someone on the street, and the insider, the person that is legally working there that suddenly decides for his or her own reasons that he is going to do something wrong or illegal, and he is going to attempt to do it in a clandestine way. So, a knowledgeable insider attempting to remove an agent falls into this category. You can have a combination. You can have someone working on the inside that, for whatever reason, is in collusion with people on the outside, and helps them. This is a very significant level of threat because this allows me as the terrorist on the outside to have enough information to make my attack very successful.

Operational Disruption Attacks

This goes back into my favorite area where I attack you without ever coming near your facility. And why is that a good thing to do? Because even though you might have security, do the people who provide you with electricity have security? These are attacks against your support systems. These are attacks of your utilities. For example, you follow all the procedures for transportation. You give the agent to UPS or FedEx. If I steal the agent from FedEx, who is held responsible? If I steal the agent from FedEx, whom does the press blame? Those are things to consider.

Attacks against personnel away from the institute: You may know about the case where someone, knowing what went on in a facility, showed up in the morning GW Turnpike rush hour with an AK-47 and started shooting people, stopping traffic. Fortunately, that was the CIA and not a biological research institute, but can that happen in the United States? Yes, it can.

Attacks against the operational process: What happens at your institute if I somehow get inside and seed your hallways with the agent you are working on? What if I contaminate an adjacent laboratory or another facility or a classroom at a university with an agent you are working on? The resulting furor and investigation will certainly shut down your operation. What are your vulnerabilities? Openness. Practically everybody in this room does open, scientific research. That means people know what you do, people know where you are. It's not a secret. That makes you vulnerable.

Visibility

This is similar to openness, but this means how visible you or your assets are to a threat. There was a good example of a low tech way of reducing visibility that I heard earlier today, and that is: Do your vials say, "Warning! Don't touch this particular vial because it's dangerous." Or do they all have similar, relatively innocuous labels? If you take a facility and you put a barbwire fence around it today, and it didn't have one there yesterday, the terrorist goes, "Hmmm. Maybe there is something in there." In fact, the more security I see go around a site, the more likely I might think that there is a valuable target in there. Visibility can become a vulnerability.

The more visible you are as a target, the more likely you appear on somebody's radar. Which scientists in the United States working with select agents might be the most likely to be attacked if somebody wanted to attack a scientist? Guys whose names get in books. The more times they are in a book, the more likely they are to become a target.

Facility Design

Almost every biological facility in the United States was designed as an open academic laboratory. The BSL Suites are generally fairly well protected, at least from a safety standpoint, but the rest of the facility is pretty much open. I know that because when you try to go and retrofit security to a lot of them, it's very difficult. But that openness, the use of glass, the use of open space, and all those things we like in our facilities, increases our vulnerability to attack. If one of the threats we think we have is a car bomb, it does not make much sense to put an entire glazed front on a facility.

Security Methodology

How your security is done or not done may be your vulnerability. Having been a security guard, I can tell you people fall into ways of behaving and bad habits. You may have guards searching vehicles at the entry control point, and they may be sweeping a mirror underneath the vehicle to look for bombs. They see hundreds of vehicles. My experience as a terrorist tells me, in most cases, I could put a bomb under there and they would not see it. And I hate to tell you that my experience as a simulated terrorist revealed that if I paint it red and write B-O-M-B on it in white letters, they still might not see it because they have fallen into the habit of seeing what they expect to see. Putting guards and fences around the outside of your facility may make you vulnerable to the insider threat in a couple of ways. One, now you have your focus on this perimeter. You don't have your focus inside your laboratory. Two, you've spent a lot of money on a fence, and it doesn't leave you enough money to spend on insiders.

Security Equipment

Your security equipment might be nonexistent. Your fence might not stop vehicles when it is sup-

posed to. You might have a fantastic alarm system, but... You might have a state-of-the-art entry control system, but you have so many entry points and so many alarm messages coming in at one time that your central processing units have a message queue length of a minute and a half, which means when the alarm comes in, instead of instantaneous display, it comes and sits in that queue. Being a terrorist, I love that because it's a minute and a half from whenever I set off that alarm until the guard even knows about it.

Operational Weaknesses

Not only might your security force fall into bad habits, but your operational people might as well. Your receiving department, how well do they check packages? How many packages do they receive? How well do they follow the procedures they are supposed to follow when they receive packages? Can I send a package to your facility addressed to a specific individual and it goes to his desk without screening? As a terrorist, that's a nice thing to have, and it is very common.

Planning Methodologies

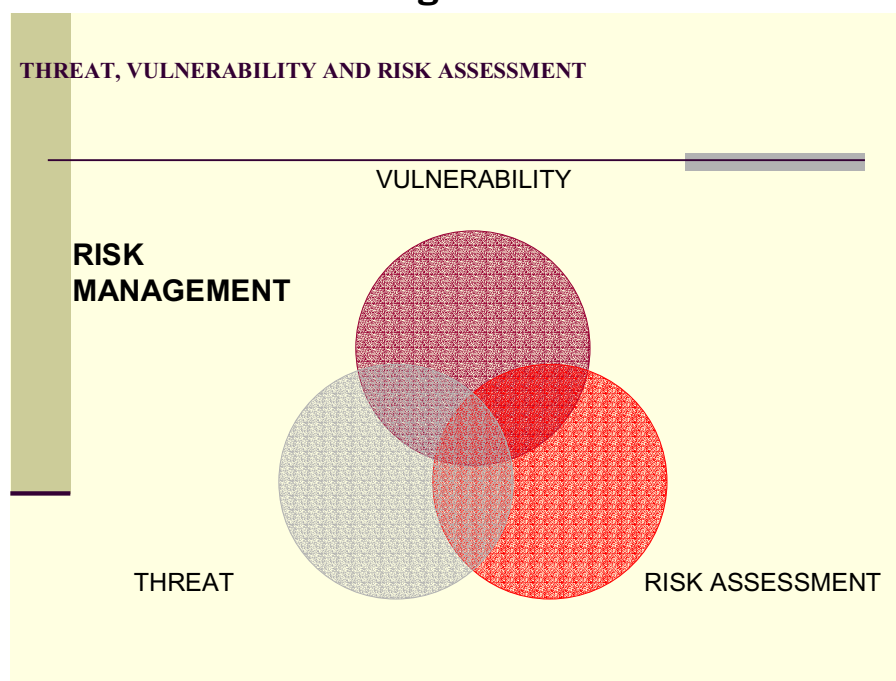
Okay, what do you do against me? How do you plan to deal with me when I show up at your facility?

There are two basic ways of doing security planning. One method is to plan for each specific threat. The other is compliance-based. Somebody gives you a set of guidelines, oh I don't know, maybe a CFR or something like that, and tells you the things you need to do, and that they are going to come and inspect you and see if you are doing them. The smart way is to combine the two methods because if you look, for example, at the current CFRs, most of what they mandate is documentation, planning, authorizations, and procedures, and very little in hard security on the ground. The facility itself, the people working in the facility, still have to decide how they are going to implement the security on the ground. If the CFR mandates access controls, you still have to decide what your access controls are going to be and how you are going to use those access controls to deal with the threat.

Risk Management

This is when you take that risk assessment and you say, "Okay, this is my risk. How likely are these things to happen? What might happen? What can I do to address it? If these are my threats, and this is my pool of resources I have available, where do I align my resources against the threat to get the best

Figure 1



bang for the buck?” Because there is no one, including any government organization that has all the money in the world they need to address every security threat, I don’t think there is any facility represented within this room that has the capability of mitigating, to any significant extent, a Boeing 767 crashing into the building. So, you make a decision about what threats you will deal with and how you’ll deal with them.

Risk Assessment

This is when you look at what your threats are, what your vulnerabilities are, and you assess: “What is my risk?” If you have a threat of an armed outsider and you have no access control and you have an open door, how high is your risk? If you have an aircraft flying around and it’s going to crash into your building, how high is your risk? This is a management decision. This is a decision made within the facility and organization with the help of security professionals, but hopefully, with major input from the folks who work there, because this is the thing that you are going to have to use to plan.

Likelihood of the event. How likely is that particular event? What are the consequences of the event? For a very unlikely event that is catastrophic, how much does that weigh against a likely event which has negligible influence? That’s the decision. How likely is it for any threat? If I’m the terrorist, do I have the opportunity, capability, and intent? Opportunity is: “Can I actually do what you are worried that I might do?” If what you are worried about is an insider stealing an organism and I am the terrorist, I have opportunity only if you let me in. Do I have the capability? That is a judgment call. Am I capable of carrying out the event? The hardest to deal with is intent. When the FBI hired Robert Hanson and the CIA hired Aldrich Ames, were they able to judge their intent? At the time both were hired, if you could have judged their intent, I don’t think you would have found they intended to be spies for a foreign power. But since none of us can read minds, it’s very, very difficult to judge intent. This is one of the problems intelligence analysts have when trying to address a threat or tell somebody what might happen. Unless that person comes forward and says, “I intend to do this,” we don’t know. What has oc-

curred in past? How many laboratories here have had a theft by an insider? That goes to address likelihood of any risk assessment. If it hasn’t happened, how likely is it to occur? You could throw that back at me because on September 10, 2001, how likely was it considered that somebody might crash an airplane into a building?

Consequences

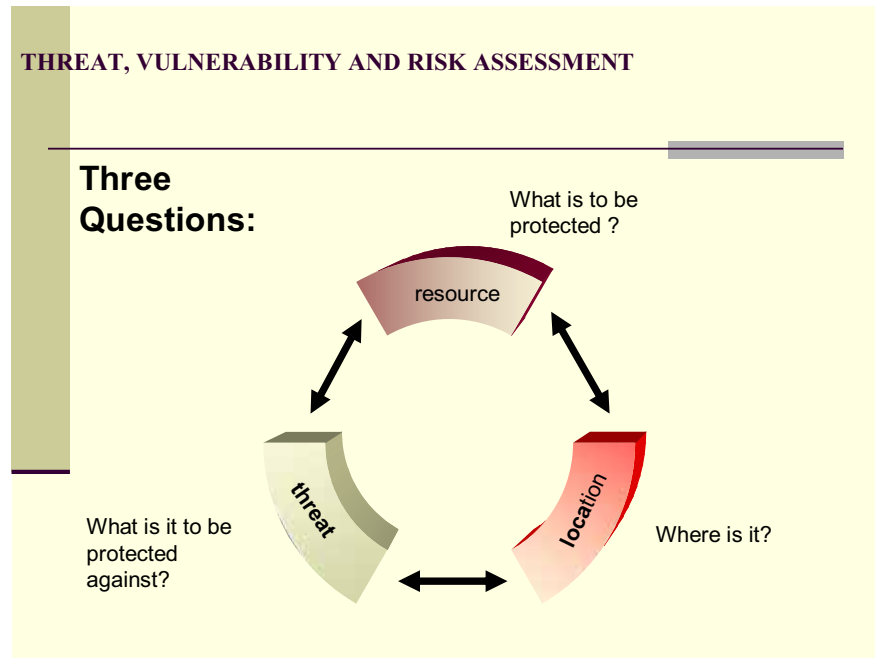
Monetary costs. Operational costs. Social costs. If you have a major event of a hostile nature at a laboratory containing select agents, the most significant one of those will be the social costs. Because what is going to happen then is going to be massive disruption to your operation and the operation of everyone else and the ability to conduct this kind of research. The monetary costs and the operational costs would be significant, but not necessarily the killer.

To do a risk assessment right, there needs to be cooperation between security professionals and operators. And you need to have feedback among all elements. Quite often, I see assessments being done where people come to a place, they walk around, they look at it, and they talk to maybe the safety people, if the facility is lucky. They talk to some senior people, but never once go out into the laboratories and talk to the workers. They don’t talk to the custodial staff. They don’t talk to the guards around the outside or the police that deal with the community adjacent to the site. As a result, they don’t get all the information that they probably need to make a good assessment.

Risk management is mixing the threat, the vulnerability that we find, and the risk assessment and putting them together in a matrix to tell us what threats we’ll address, how we’ll address them, and how much we are willing to spend to address those threats. But also, and more importantly, how much risk are we willing to accept, because life without risk is impossible.

We look for measures to prevent an event, measures to mitigate an event, and measures to recover from an event. For example, let’s talk about an airliner hitting the building. I’m not expecting you to be able to prevent it, but as a society, I would expect you to be able to tell me what was in your building after the airplane hit it. Are all your records and data

Figure 2



stored only in one facility at one place, so it can all be knocked out at once? If the responders show up to a major fire at your facility, are all the records that would tell them what is in there and where it is located in that same facility? Risk management is a decision by the operator, the laboratory, the people doing the work, the supervision, and the folks responsible. What is it we are willing to do? What is it we can do? And what is it we are willing to accept?

Some Guidelines

Security measures should never impede the operation that you are doing, and there is a reason for that. If I'm the terrorist and I can make you do security procedures that stop you from doing the work you are doing, then that's as effective as actually going in, personally, and stopping you from doing the work that you are doing. Or, if I make you put so many guards around something and so many locks on it that you can no longer work on it, I have achieved my goals. Also, if the security is an impediment and it gets in the way, people have a way of dealing with impediments. We all know this. We all use them in our lives everyday and they are called "work arounds." If I put such restrictive requirements on removing an item from a freezer or a stock

culture that it makes it very, very difficult to work, how much does that increase the chance that a researcher or someone else in the laboratory will maintain a bootleg stock of culture somewhere? If my measures make it too hard to comply, what happens then to my insider threat? In other words, I've created more of a problem inside the facility than I've helped.

You the operator know more about how to secure what you do than I as a security professional would ever know. If I come to you and I say, "What could someone do to hurt you?" you can probably tell me better than I'll be able to figure out on my own. You may not tell me what the effects are of a 20 lb. explosive device as opposed to a 50 lb. explosive device, but you can tell me the consequences of what would happen if there was such a device. You could tell me the consequences of what might happen within your facility. You can tell me where your doors are probably weak, where your operation is probably weak. As a professional, that is something that I really want from you.

If you are involved in the process, you know the old buzz word "buy-in." If laboratory workers are involved in the process, that makes them feel part of security. What catches the insider, what lets us know

about illegal insider activity, are the workers who work around them. In the case of Hanson and Ames, for quite a while before they were caught, it was folks who worked around them who said, "There is something weird going on here with these guys." These are people who passed all the personnel reliability stuff we have available in the U.S., but turned anyway, and they were identified to us first by people who worked with them. That's the result of getting the operators involved and getting them to participate in security and see security as part of what they do rather than a set of onerous guidelines and directives imposed upon them. If you provide the security for whatever it is you are working with, it makes it a lot more effective and a lot cheaper than having some program imposed from above by another organization.

There are three questions to ask, and they are simple questions, but the answers are not so easy.

1. What is it we want to protect?
2. Where is it located?
3. What do we want to protect it against?

Basically, our measures against the threat are these: For every threat that we identify, we want to have measures that might deter the threat, might detect, delay and channel it, assess it, respond and neutralize it, and recover from it. When you have a set of threats, you need to think about each one of these measures against each one of those threats. The things that work against a knowledgeable insider are not the same things you would use to work against a casual person who wanders down the hall in a laboratory and might walk into a secured area. The things that you might use against a hostile intruder armed with a handgun are not the same that you would use to deal with a truck bomb. For each threat you develop a security plan to meet those objectives against that threat, and you evaluate it realistically against that threat.

Some objectives against some cannot be met. Deterrence is a nice thing. We think if we put a fence around the place, it deters. If your threat is an armed commando force, what are you going to use to deter them? There is nothing that will deter them. They have been assigned a mission. Your security measures rather than deterring them become an impediment, and they just plan around them. How do you

deter somebody from wandering down the hallway of a university laboratory and walking into an area that contains select agents? Perhaps a door lock and a sign. Some threats you can deter. Some threats you cannot deter. Please be aware that deterrence is in the mind of the terrorist or perpetrator. It is not in your mind. So, what deters you does not deter them. What deters a normal, rational human does not deter a distraught, disgruntled person who shows up at your door.

Below is a matrix. For each threat, we talk about the target. We talk about the threat itself, the vulnerability, how likely it is, what the costs are, and then what actions you might choose to take. In this example, an anthrax culture in an incubator, the threat we are worried about is an insider. How vulnerable is it to the insider? How likely is it? What would be the cost if it occurred? What measures am I going to use to mitigate that threat?

Or as you see, in this case, deterrence and detection. I'm primarily concerned with what we call "Personnel Reliability Program." This is knowing who works there and having the coworkers know who is working around them, and how they are acting. You need to develop your anticipated threat, based on what you actually do. And I say this: Are you reasonably a target for a huge terrorist attack? If you are not, don't plan for huge terrorist attacks. If you work in a diagnostic laboratory, is your operation less of a target than if you worked in an advanced research institute? Are the amounts of materials you deal with significant enough to make you a target? You plan your security measures based on the threat that you have decided upon. One of the problems we have as a country is that we really don't have a good handle yet on what exactly we should be worried about. We all have some ideas, but everybody you talk to has a slightly different take.

You should exercise and evaluate your security program against the threat. It's nice to have inspections, but I know of many military units that pass inspection after inspection, and yet if you came in and acted as a terrorist, you could get right through their security measures. There is a difference between inspecting and exercising the security measures. A good example is: We know in the United States that there is a threat of explosive devices and

Figure 3

THREAT, VULNERABILITY AND RISK ASSESSMENT

target	threat	vulnerability	likelihood	cost	action
<i>B. anthracis</i> in culture incubator	Theft by insider	High, numerous personnel have access	Unlikely	Shut down of lab, loss of life, terrorist attack	Deter: Personnel reliability program Detect: Personnel reliability program, operational monitoring Delay/Channel: Access Control measures Assess: Monitoring, inventory control procedures Respond/Neutralize: Security force, law enforcement Recover: Stock cultures, records

weapons being smuggled onto airliners. We know that it is likely. We know the cost of it, and we have developed a set of things to mitigate that risk. We have exercises. How do you check to see if your measures work against smuggling guns on an airplane? You try to smuggle a gun on an airplane. But just because you exercise it, how do you evaluate it? Does anybody know the success rate of the tests of smuggling weapons through TSA onto aircraft at this time? In other words, the government evaluators who were sneaking guns on airplanes, how effective are they at getting them through? They are a lot more effective than we would like. So, if you have security measures, test them. It is easier to test ahead of time, when you are in control, than have it tested by me as the terrorist at some time of my choosing. You have to make this evaluation and test fair, and you have to make it without retribution.

One of the problems I had in penetrating nuclear weapons security was every time I penetrated it, the poor kid that was standing there got disciplined, even if I penetrated it through no fault of his or because he “failed in his job.” If you have a guard force that makes a mistake during an evaluation and you fire them, what you’ve done is fired the most experienced folks you have. If somebody sends a SWAT

team to get into your building, they’ll probably get in because they are trained to do that. If somebody sends the SEALs to test your security and they don’t get in, we need to stop paying the SEALs because we’ve trained them to get in. What we need to do is use that as a learning experience. When we evaluate, we need to use it as a learning experience not a disciplinary experience. In a lot of cases, we try to fix blame instead of fixing problems. If you tell me that your security measures are effective, my answer is, “When is the last time they were tested?”

You have to be careful about applying other programs. Linking biological research materials with weapons of mass destruction leads us down a very, very poor path towards security. And the reason I say that is it is really hard for you to go into a nuclear storage area, put a nuclear weapon under your arm and walk out with it, for a lot of reasons. The same is true of chemical weapons. We link biological agents used by terrorists with radiological and chemical agents, but there is a difference in the security between a weapon, which is an end item that is normally in storage behind lock and key and not normally accessed, and materials held out in the open for research purposes.

In nuclear security, we do not go to Fermilab in

Batavia, Illinois and tell those scientists who work on the accelerator that they'll have to account for every particle they generate. First off, they'd quote some guy named Heisenberg and tell you to go away. But secondly, we don't do that, because guess what? They are not working with weapons. Can the knowledge they are developing there be used for weapons? Yes. Can some of the materials they use be converted into weapons? Yes, but they are not weapons. The same is true of organisms being used for research. So, you have to be careful. Things designed to do one thing don't necessarily transfer very easily. An example in biology is the requirement to do exit inspections at facilities because we think someone's going to carry out the agent. Searching the briefcase of everybody leaving the facility every day does nothing to stop a knowledgeable insider from carrying an organism out of the building. It looks good, but if we think about it, if we are not searching the guy's pockets, what stops him from putting it in his pocket? What stops him from applying it to his hand? You can say, "Yeah, we are doing exit inspections, but how effective are they against the threat?" If I put on my terrorist hat, I laugh. Ok, search my briefcase.

We have inventory controls. At one point, I know, people were saying we had to account for every microorganism. As microbiologists, we all go, "Very funny. I can't even tell you how many are in this one tube because guess what, oh, one died today." And there was a requirement to record the destruction of every microorganism, and it was like, "Well, what happens when they die on their own?" You get what I call the "deer in the headlights look" because nuclear materials do have a decay rate, but the bombs don't die on their own. The chemicals don't die on their own. But, if you leave a tube in an incubator long enough, everything in there is dead. There are some very significant differences.

There are some pitfalls that we all fall into. My favorite is the mosaic versus the big picture. If you get far enough away from a mosaic, it looks like a solid picture. If you are at a high enough level in the government or any organization, it looks like you see the big picture. But, there is no big picture. There are thousands and thousands of little tiny pixels. One pixel might be letting box cutters on an airplane. Another little pixel might be that down in

Phoenix, there is an Arab immigrant taking flying lessons who doesn't show much interest in landing or taking off. Another pixel might be all aircraft hijackings result in peaceful landing of the aircraft and sometimes hostile events, but usually the release of the hostages. If you move back far enough, you don't see any of those pixels. You see one nice big rosy picture. But, we know now because of hindsight, that those pixels mattered. The same is true in any security program dealing with anything. We have to be very careful that by looking at the big picture, we don't miss some very, very significant small details.

Threat is a guess. Intelligence is a guess. We hope it's a good guess, an educated guess, but it is a guess. It's a guess about what is going to happen in the future. We all like to think we can predict the future, and for most of us, our past lives and what happened yesterday do give us an indicator of what might happen in the future, but ultimately, there is no guarantee. We think we know if we leave this room and walk out there and walk across the street, we'll be fine. We don't imagine that we will walk out there and be struck by a car, but there is a statistical chance that if you cross that road you will be struck by a car. Things change. You didn't predict it. All terrorist acts cannot be predicted. It is easy after an event to put together that little chain of data points to say, "Oh well, we should have seen this. How stupid were we not to see this?" Well, it's easy now to connect the dots backward in time. It's not so easy to connect those dots going forward because each dot has so many other permutations. The farther back in time you go, the more permutations you have at the end. So, you might guess right, but you might guess wrong. Intelligence is a political product, and by that I mean politics with a small "p" because it is a product of a human bureaucracy. We've seen how intelligence may not necessarily be correct. It may not be wrong. It just may be slightly incorrect. It can have very large consequences.

Group Think

This is where we make a decision that we'll all think the same, that if our threat is the insider that we will say, "Oh well, we will go worry about the insider." If our way of dealing with the insider is this, we'll all deal with the insider this same way. But,

what about the critic? What about the guy in the back of the room who raises his hand and says, “But, but, but, but, but. Sir, excuse me. That won’t work because of this, this, and this.” What do we tell that guy? Do we tell him to sit down and shut up and do what we tell you? He is doing for free what the terrorist is going to do to you at great cost. He is pointing out potential problems. If that guy in the corner can see problems with your security or your operation, somebody else might see it. There is nothing wrong with listening to dissent. The more eyes you have, the better the chances are that you won’t miss something. Now, just because he sees a problem with how you are doing it, doesn’t mean you have to stop how you are doing it, as long as you take that into account when you make your decision. Everybody had an opinion and maybe not all points of view can be put into the final product, but let us not silence the critics who might be the guys telling us what we want to know.

If someone in your field offices tells you, “I think somebody’s learning to fly airplanes for nefarious reasons,” let’s not shut down that voice. If we

have somebody in a laboratory saying, “You know, it’s great to have all these security measures, but I can still smuggle the organism out this way,” let’s not tell him to shut up and just do what we are telling him. It is important to allow that kind of criticism. When you evaluate your security program over time, you need to incorporate those things you learn through that criticism, in the changes that you make. Wishful thinking. We all would like a nice safe place. We would like life to be very comfortable and without risk. We would like to think that we can throw a security fence around a building and we are suddenly safe. If we silence the criticism and we continue to indulge in wishful thinking, we set ourselves up. We set ourselves up for a very dangerous fall because we’ve assumed, “Okay, we have these security measures in place, and they’ll deter the terrorist.” Maybe they won’t.

That concludes my presentation. I hope I’ve given you some food for thought, and I hope to hear some feedback, and I hope to not catch too many spears.