



# Understanding Security Basics: A Tutorial on Security Concepts and Technology

Richard Kibbey

Science Applications International Corporation, Melbourne, Florida

## Author's Note

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

Although this article presents an overview of security concepts and systems, you will still need a security expert, either from your own organization or outsourced to a full- or part-time contractor, to review the security plan for your facility. A security expert has the experience to help you implement a security program that covers all the elements of security and allows you to put the right components in place.

Our discussion begins by drawing you a mental picture of a probable threat element (PTE). Groups of PTE are located throughout the United States. It should be no surprise that they are plotting operations against us all the time, even today. Consider this scenario: Field members of a terrorist organization meet in Baltimore in December 2002 for an initial meeting. Two of them are from New York City and two are from Fort Worth. Their mission? Steal biological material for a bioterror attack on the U.S. food supply. They meet again in March 2003 at the Black Angus restaurant in Atlanta to discuss target selection. The men decide to conduct pre-selection operations at three locations: Centers for Disease Control and Prevention in Atlanta, the U.S. Army Medical Research Institute of Infectious Diseases (USAMRIID) in Fort Detrick, Maryland, and Plum Island Animal Disease Center in Long Island, New York. Surveillance on these targets is conducted from April to September of 2003. The purpose was to identify weaknesses in security to exploit during

their operation. The criteria were to find a location that had poor lighting, weak CCTV cameras/systems, and an inconsistent access control system.

They began their surveillance of the CDC in April to June 2003. They recorded their observations and discovered that there were new alarm systems at the CDC and numerous high-tech television systems strategically located throughout the complex. The site is also patrolled regularly and there were barriers that could hinder movement. Their assessment was that the security components hindered the proposed operation and made it extremely difficult to continue their pre-attack surveillance.

In July and August 2003, they conducted a surveillance of the USAMRIID. The tactical information collected revealed similar problems. A large number of uniformed personnel made them very nervous. It just so happened that during their surveillance the USAMRIID was conducting an anti-terrorism threat exercise, which also made them nervous. Additional security measures made it even more obvious that this site was well protected. There were many lights and security structures. They used barriers during the exercise. There were consistent access control procedures, not only at the building but also in the streets leading up to the building. In addition, there was a visible use of guards and posts. Their assessment was that this location was too difficult.

In August through September 2003, they conducted their surveillance on Plum Island. Here they found what they were looking for: Numerous gaps in security, security doors left open for ventilation,

**Figure 1**

Hypothetical Scenario

**Dec 2002**

- Four members of HAMAS meet in Baltimore, MD
  - 2 from NYC, NY
  - 2 from Ft Worth, TX
- Their mission: Steal biological materials that can be used in a bioterror attack on the US food supply



NOTE: Map from the testimony of Steven Emerson 2/24/98 to the senate judiciary subcommittee on terrorism, technology and government information.

**Figure 2**

Hypothetical Headline

**New Headlines**

The CDC announced today that a major crisis has developed in the US beef industry...



Major Outbreaks of Mad Cow Disease  
Beef industry collapses

some windows left open overnight, alarms and door sensors not operational, and poor lighting, both interior and exterior to the facilities. The site also had inadequate and broken CCTV equipment and inconsistent access control procedures. As a result, the terrorists selected Plum Island as their target.

September through December 2003, they conducted their pre-attack surveillance. In this phase, they discovered a route of ingress based on good terrain and shadows and darkness for their approach. They also found a point of entry—a window in one of the buildings that they wanted to access that was left unlocked most evenings. After observing daily operations for a period of time, they selected their target. Note on the slides that they designated points on their maps where they were going to attack and what they were looking for.

Early in January 2004, they conducted their operation. One individual remained at the vehicle approximately a half a mile from the site. The other three followed their attack plan and entered the building at a poorly lit window. They made their way to the laboratory and easily gained access by bypass-

ing door alarms by cutting a hole in the drywall. They located several vials of hoof and mouth virus and exited the same way they entered. The entire operation took less than 70 minutes and the whereabouts of the perpetrators and the missing virus is unknown—until...[Laughter] the CDC announced today that a major crisis has developed in the U.S. beef industry.

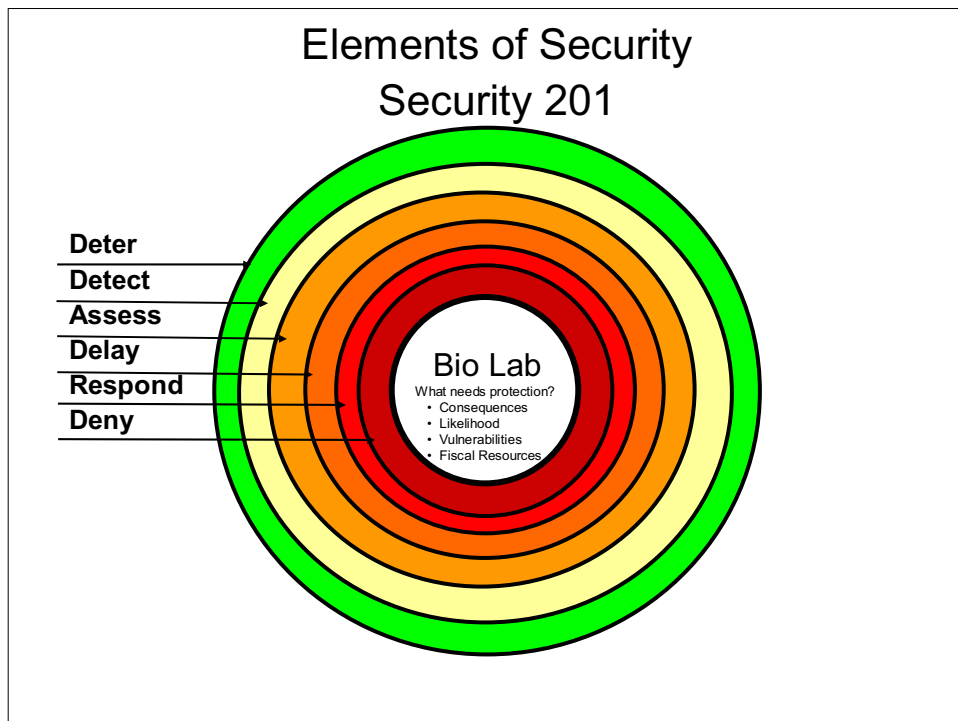
The situation I described is a hypothetical scenario, but it does have real world consequences if it should ever happen. In fact, the security deficiencies I discussed for the target location were identified in a recent assessment.

So, how do you avoid this at your facility? Well, hopefully, I'm going to give you at least a direction to go in to get the answers. Consult your trusty, local security expert. This guy may not look like he knows what he is doing, but a properly trained security expert with experience can help you provide your facility with a cost-effective and efficient security program. She or he can help you improve or develop a sound program, and here is how.

I look at a security system as having elements.

**Figure 3**

Rings of Security



These are rings of security that go around the resource you are trying to protect.

Each of these rings is an element of security. Each is supported by security equipment and security procedures that will either deter, detect, or support defeating an adversary by being applied to one or more of the rings of security. These are the components of security. So remember: Components equal electronic equipment, procedures, and processes, and elements are the rings. We are going to discuss those rings right now.

The rings are Deter, Detect, Assess, Delay, Respond, and Deny. Everything in security should apply to one of those areas. If it does not, you are spending a lot of money without getting very much help. The first question to ask is “What needs protection?” What do I have in my facility that needs a security system? Then, after you’ve figured out what it is you are trying to protect, you need to know how much of it there is. Is it a cold virus? Is it Ebola? Is it a hoof and mouth virus or something like that? The lower on the risk scale, the less equipment and sophistication you need. The higher on the scale, the more security you are going to need. The amount of security you need will be determined by determining what your threat is, the vulnerabilities that exist in your facilities, the likelihood of an attack, and the consequences should an attack occur at your facility.

- **Deterrence** is the prevention of action through a fear of unacceptable consequences, as viewed by the PTE. It is not a physical state. It is a psychological state that your security program gives a perception of, from the outside looking in. If the PTE perceives a risk of being caught, he will usually move on to another target just as in my scenario where they looked at two locations. One was too tough, so they went somewhere else. It’s unfortunate in our business that when we are dealing with deterrence we say, “Let’s keep them away from here” and you end up sending them somewhere else. But, if everybody is doing his or her part, you are going to make it very difficult for an adversary to be successful.

- **Detection** is the determination and transmission that an event has occurred. The use of technology increases the capability to detect. Ideally, you will detect as far away from the resource as possible. Assessment is the analysis of an event by a person di-

rectly onsite or via technology—usually today a closed circuit television (CCTV) system. Assessment is necessary to determine the validity of an alarm and an appropriate response.

- **Delay** is the ability of physical or psychological barriers to restrict movement. The purpose of delay is to allow time for an appropriate response and to make it undesirable for the perpetrator to continue.

- **Response** is the level of reaction required to counter an intrusion. Response forces range from unarmed security guards or staff to local police. At the high end there are dedicated armed response forces like you would expect to be around nuclear storage areas.

- **Denial** is the ability to oppose or negate the effects of an overt or covert action. Denial is the final and last chance to defeat an adversary.

Now we are going to discuss the components of security. Components of security consist of equipment, policies, and procedures that support each of the previously discussed elements (rings of security). The components consist of clear zones, barriers, lighting, shrouds, locks, electronic security systems, access control systems, guard forces, and operator/owner procedures.

- A **clear zone** is usually provides a 30-foot clear zone from the facility or object you want protected. It is void of trash receptacles, dumpsters, ashtrays, brushes, and other objects that could obscure a small bomb or provide cover to an adversary.

- **Barriers** are designed to restrict, deny, or channel pedestrian or vehicular traffic, and in most cases, will do the same for potential adversaries. Barriers are not necessarily impenetrable but they do increase the probability of detecting people and vehicles or dissuading them from attempting to illegally access your location.

- **Lighting** is a significant deterrent to potential intruders. It enhances visibility for routine patrols and general staff and allows response units to have better visibility. Permanent lighting should provide adequate illumination to entry points, site perimeters, pathways, and parking lots. And you can have lighting that is activated by sensors—motion sensors or line sensors—that will activate the lights when they are penetrated. These can be activated by timers or operated manually.

- **Shrouds** are an often-neglected component of security. They support deterrence and delay by providing concealment from chance and direct surveillance. The purpose of a shroud is to limit visibility from unauthorized sources. It can be as simple as darkened windows or curtains or a more complex structure such as walls, coverings, and even shrubbery.

- **Locks** come in many shapes and forms, from single hasp locks that you have at your house, to very complex systems. They include standard key locks, combination locks, cipher locks, card access control systems including swipe cards and proximity cards, seals, and biometrics. All of these can be tied into an electronic security system, if desired.

- **Electronic security systems** come in three flavors: access control, security surveillance, and intrusion detection. Access control systems include devices designed to limit access to a site, building, room, and containers. They can be very complex systems with biometrics, exchange badge systems, and other electronic devices, or they can be a simple card swipe access system.

- **Security surveillance:** The most common surveillance system is the CCTV, which is offered with a variety of capabilities. This is one area that I would caution you on. You will have hundreds if not thousands of vendors telling you, "I've got the camera for you." You need to be extremely cautious regarding what kind of system you buy. When choosing a CCTV system, consider the resolution and the image quality. Do you need color or black and white? Is pan/tilt/zoom capability what you want the camera to do for you? What type of transmission mode do you need? That includes fiber optics, coaxial cables, and wireless. Other considerations include light levels and weather.

- **Intrusion detection systems (IDS)** identify unauthorized entry. Usually, they are connected to a monitoring system of some kind and fall into three general categories. (1) A local alarm system, which, when the IDS is breached, sounds an alarm for a local security officer or staff to respond to. (2) 24-hour central stations that are usually commercially operated. When they get an alarm, they contact the local police or a designated security service. (3) Proprietary alarm systems are controlled and monitored

within the facility. This system usually reports to an onsite security control center and response is provided by an onsite security force or local law enforcement. Intrusion detection systems can be specific right down to a room or a container. They can be simple alarm systems such as ADT home alarms or more sophisticated systems that include CCTV, access verification, and other technology. Intrusion detection systems consist of sensors, which can be motion sensors, glass break sensors, and contact or beam sensors. Transmission components include coaxial cable, fiber optics, and wireless. Most IDS have an alerting system that usually terminates at some kind of monitoring function.

- **Guard forces** or response forces need to be considered in your security system. There usually needs to be a good balance between the use of security technology and a properly trained security force or staff that has security response responsibilities.

- **Owner/Operator** procedures are the one thing that you have complete control over and won't have to spend very much money on to improve the security of your facility. This is all internal and consists of written procedures and processes that your organization must follow. These procedures translate policies into action for people responsible for carrying out those instructions. Security policies must be backed by well-defined procedures. The next two slides list several policies that you should have in writing at your facilities. In my scenario, I talked about leaving windows open. I worked in several areas in the military where we were supposed to lock up at night, and in the morning we'd come in and find windows wide open. It happens all too often. So as a minimum, I recommend that the following written procedures be implemented at your facility:

- End of day security checks
- Computer procedures. These are very important to keep your information secure and out of the eyes and hands of somebody who would want to do harm.
- Access to restricted areas
- Visitor and contractor procedures
- Escort requirements
- Property passes (removal equipment)
- Parking restrictions
- Personal and vehicle restrictions

**Figure 4**

# Probability of Protection

Low Risk  High Risk

	1	2	3	4	5
Visual Assessment Tools	Partial coverage by fixed CCTV	Total coverage by fixed CCTV	Above ground Observation towers	CCTV w/pan, tilt, zoom	Video motion detection, thermal tracking, IR capable
Electronic Security Systems	Perimeter alarms	Perimeter and asset alarms, ID checks	Automated access control system	Access control system w/biometrics	Dual line security systems, exchange badges, container access control
Barriers	Signs, simple fences, ditches, shrubbery	Berms, fence, wall	Fence w/cable Fence w/outtrigger	Bollards, jersey barriers cabled	Barrier & fence system plan, ability to engage
Structures			Stand off distance delineated	Walls/roof reinforced,	Doors windows ballistic resistant, HVAC filtration capable

So far, we've looked at the six elements of security and numerous components of security. An effective security system will incorporate a security-in-depth concept by employing some or all of the elements of security. These must complement one another, be integrated, and work from the resource out to the perimeter of your facility. This will provide you with a solid program that mitigates the level of risk and the vulnerability of your facility. Figures 4 and 5 are a matrix of components and risk levels.

These simple matrices illustrate the components of security that you might consider implementing at various risk levels. Left to right, the security components become more complex. You can buy CCTV

cameras as cheap as \$150 per camera, or you can buy them as expensively as several thousand dollars per camera. For a simple lab that has very little risk and very little consequence of losing sensitive resources, a simple ADT-style, commercial system is probably sufficient. When you get up to facilities that are doing weapons-grade bioresearch, you will need something a lot more complex. The second slide has a few more examples covering some of the elements where you can start at the lower risk level and move your way up. The combination of security components that covered by the elements of security, constitute the level and depth of protection you have at your facility.

**Figure 5**

# Probability of Protection

Low Risk  High Risk

	1	2	3	4	5
Locks	Warded	Disk Wafer	Pin tumbler	Super pin tumbler	Lever, high security lock
Shrouds	Covered from chance observation	Covered from direct observation	Covered from ground observation	Covered from space observation	Total cover to include protection from attack
Guard Force	Local Law Enforcement Only	Unarmed Part Time	Unarmed Full Time	Armed Part Time	Armed Full Time
Clear Zones	Outer perimeter only	Inside and outside outer perimeter	Clear zones for all sensor fields	Lighted	Lighted and alarmed, delineated by type 2 fencing
Lighting	Handheld lights issued, temp lights during higher threats	Building exteriors lighted	Sensor or timer activated	Gates, and entry points , all clear zones	Restricted and critical areas, entire site illuminated