

The Terrorist Threat You Face in Managing the Security of Radiological Sources

D.T. Coulter

Your concern, and rightly so, is “what is the real threat to my facility, devices and radioactive materials that I must protect against”. When I visit sites to assess risks, my first question is “what is the real threat to this facility”. I need to know the threat before I can identify the vulnerabilities, probable consequences and resulting risk. After all, we are in the risk management business, and without the threat we are unlikely to identify the true risk(s) you face.

The DHS terrorist threat condition is presently “ELAVATED”, which means different things to different people. The exact definition of elevated is not as important as the fact that we should be at a heightened state of security awareness. That’s difficult to do when you consider the “half life” of security awareness ranges from thirty to one hundred and eighty days depending on the severity of the security violation...and don’t forget the annual hand wringing that accompanies the anniversary of really catastrophic events.

The intelligence community's daily threat assessment, developed after the terrorist attacks to keep policymakers informed, currently lists, on average, 25 to 50 percent fewer threats against domestic targets than it typically did over the past two years. Is this because of something we are now doing, something we did, something said...or do we know. My guess is we don’t know...gathering data and turning it into intelligence is more art than science. So when I walk into your facility and tell you I’m there to conduct a security assist visit...what am I actually doing? I am assessing the risks you may be facing predicated on a defined threat after uncovering “gaps in security” or vulnerabilities, because we can all guess what the consequences will be.

If I come into your facility and disclose that the threat you are facing is a group of al Qaeda terrorist that may want to steal your high activity radiological source from a two ton device you have behind a locked door...your thinking, OK...I will be polite...I will be cordial...but what is this guy...NUTS. In fact I can’t say that...in fact, I really can’t say anything about your threat because I don’t know what it is. You, your staff, your management and your security force are much more likely to know what the threat is to your facility or organization than anyone from outside the organization.

Now here is where it gets tricky...you control your perimeter, meaning everything from your parking lot to the threshold of the building to everything inside your building(s). You know your facility. If on the other hand, your local law enforcement agency gives you a heads up as to something that may be going on in your area...I would pay very close attention to what they have to say. I’m not too worried with what the federal government has to say...unless it is the warning of a catastrophic type of event that they know is immanent.

When I visit a site and ask “what is the threat to your facility and high activity radioactive materials”...I normally get a blank stare from the Radiological Safety Officer (RSO) and a confused shrug from the facility security officer or the head of the police or response

force. By the way, this is not the time to have the philosophical discussion regarding threat and why they should know it...it's the time to assess the risk facing your facility. If we are honest with ourselves, we would admit that there is little to no risk of the radioactive material that we have at this facility being stolen or sabotaged. At this point, I do what I always do in this situation...I assume what the threat will be.

For the purposes of this discussion, let's say we want to protect a cesium irradiator. What can the bad guys do? They can steal the source or they can destroy the source as an act of sabotage either in the room housing the device or somewhere in or on the facility. If we apply our defense in depth methodology, we want to **detect** the intruders, **delay** them from removing or destroying the high activity source, **respond** too, and interdict them before they can accomplish their mission.

Let's take a reasonable approach to identifying the threat...not the worst case scenario or the easiest scenario...but rather the most likely case scenario. In my experience and that of most of my colleagues...there is always an insider involved. For this particular scenario, let's assume one insider and two armed attackers...terrorist if you will. Their objective is to steal the cesium source from the device to either sell it or use it in an Radiological Dispersal Device. Let's also assume that the insider is capable of getting the two attackers to the device containing the source...this is not as big a leap as one would assume. Consider everyone that could gain access to the device and go from there. If you are incapable of considering an insider threat, assume that an operator/technician going into the space that contains the device is accosted by the attackers and a gun is placed to their head to gain access to the device.

Let's assume for a moment, that two terrorist with the appropriate tools can remove a high activity cesium source from a JL Shepherd irradiator or MDS Nordion Gamma Cell irradiator in less time than you might expect (it's not an assumption...it's a fact). Let's also assume that removing the source will not provide an immediate fatal dose of radiation (another fact) to the attackers.

Now the threat scenario becomes two armed men with appropriate tools and with the assistance of an insider (or unwilling hostage) can enter the facility, gain access to the device that contains the high activity source, remove the source without short term personal injury and prepare to depart the site in less time than the device is left unattended.

I'm not saying this is the threat that you face every day... I'm saying this is a reasonable threat scenario that ***you may face one day***. Having said that...now what do you do? You must consider a package of security countermeasures that can mitigate the risk of theft or sabotage of the source. We start from the inside and work out...that is we start at the device. Efforts have been made to communicate to the manufacturers the vulnerabilities of the high activity sources when installed into their devices. Some effort has been made to make the removal of the sources more difficult (one manufacturer has added the installation of a micro switch) and therefore a less desirable target...but we are not there yet...and there are thousands of devices in place with no additional protection.

Starting at the device, attaching an anti-tampering or anti-disturbance device (ADD) is the most practical solution. A fiber optic wrap that would alarm if broken, and can never be turned off, is one recommendation...there are several others that would work just as well. The room itself should contain a series of sensors and electronic countermeasures. The sensor package should include a volumetric sensor to detect motion...you may want to install a dual mode volumetric sensor the uses both IR and microwave...both have there place. From here you must be able to control access (ACS) into the space and detect intrusion (IDS) into the space. Both systems are independent but inter-dependent. A card reader and balanced magnetic switch (or a recessed magnetic switch) on the door completes the basic package. The package can be expanded to include CCTV to assist the security force in confirming an attack and a variety of other technology to defeat the threat. The security management system just defined should be “performance tested” on a regular basis and specifically after maintenance has been performed on any of the components in the system.

This security management system assumes the room containing the device is a single use space with no windows and walls running floor to ceiling with no access outside the single entry door. If this is not the case then other precautions such as bars on windows and vents, film and glass break sensors for windows and seismic sensors to protect vulnerable wall and ceiling surfaces. The security management system should have a cellular backup to communicate alarms and an uninterruptible power source (UPS) to backup the main power supply.

Determining the threat that faces your facility is difficult but not impossible...it is a necessary first step in determining the risk. A dedicated team of senior facility management, the RSO and the facility security manager can put in place a robust security management system for considerably less then one might expect. With some outside assistance and a review of existing security policy and procedures, major stride can be easily achieved in upgrading the security of the facility to protect radioactive sources against a realistic threat.