Urban Terrorism…Are We Ready??

Douglas K. Beaver, CPP, Kastle Systems

On Wednesday, September 1st, James Jay Lee burst into the Silver Spring, Maryland headquarters building of Discovery Communications and took three hostages; two Discovery Communications employees and an unarmed security guard. After several hours negotiating with the gunman, Montgomery County tactical officers moved in when authorities monitoring him on building security cameras saw him pull out a handgun and point it at a hostage. All hostages escaped unharmed after the four-hour standoff.

Photo Source: www.policeone.com

Lee's demands were irrational - potentially even insane. He had four crude explosive devices strapped to his body. Two of them were green propane cylinders with pipes attached that contained shotgun shells. The other two were pipe bombs. One of the devices detonated when police shot him.

It wasn't the first time Lee, a homeless man who previously lived in California, had targeted Discovery's headquarters. In February 2008, he was charged with disorderly conduct for staging a "Save the Planet Protest." Lee threw fistfuls of cash in the air and paid homeless people to carry signs condemning the network. Police found his pockets stuffed with more than $20,000, according to court records. Lee, 43, had objected to Discovery's environmental programming.

In this most recent event, fortunately, none of the 1,900 people who work in the building were hurt, and most made it out before the standoff ended.

In light of the Discovery Communications hostage situation, Kastle Systems would like to offer our owners, property managers and business security managers a perspective on how to review and potentially enhance your own security posture:

1. Ensure That Your Security Response Plan is Complete, Current and Tested

Having an updated emergency plan is a central element to responding well when an attack or emergency occurs. To institute this best practice you will want to work with your security partner to define a plan with the following characteristics:

- **The security response plan is thorough**. The plan developed for your space should take into account various types of emergency events and associate each of those to clearly defined processes, which allow the situation to be handled efficiently and coordinated with all responders.

- **The security response plan is current**. It is recommended that you audit your plan at least twice a year and that your internal and external responders are provided with the most current plan, with clear indications when additions or modifications have been made.

- **The security response plan clearly defines responsibilities, and training has been conducted**. So that you respond expertly when seconds count, your people need to be familiar with and understand their role as it pertains to response procedures. Actions to be taken and responsibilities for elevated threat level situations must be clearly defined, and those assigned need to be trained. It is recommended that you provide emergency event training regularly. The best method of training is to establish a test drill to perform at least once a year. Tabletop exercises are also an effective means to ensure an elevated level of preparedness is maintained amongst employees. Together, all of these measures contribute to an overall environment of security awareness.

2. Implement a Mass Notification Capability

On April 16, 2007, a tragic event occurred at Virginia Tech that served as wake up call for college campuses across the United States. On that day, across the span of several hours, a gunman took the college hostage and killed 32 people, with many more harmed.

This event has been analyzed and re-analyzed with the goal of learning from it and applying solutions that would help to prevent and respond to anything similar in the future. A primary focus of the analysis centered on the timeliness and method of communicating with the campus community once the incident was detected.

One particular technology – called mass notification – enables this to happen more readily and quickly. Mass notification requires a system of inputs, monitoring capabilities, and outputs designed to detect threats, track events, and provide instructions to people in the presence of danger. In order to institute this best practice in your environment, you will need to work with your security partner to:

- **Develop a database of all the constituents in your environment that can be affected in an emergency situation**. The first step in mass notification is having an up-to-date and complete account of the individuals of your community.

- **Leverage advanced communication technology and utilize multiple channels of communication.** In today's world, people can be reached – and people have preferences for how they are reached – through multiple modes of communication. A combination of software, people and process can enable you to quickly e-mail, text message and call to inform people of threat and what they are to do during it.

- **Pre-prepare your scripts and instructions so you are ready when the time comes.** When an incident occurs you want to be pre-prepared. Establishing instructions for

various emergencies allows you to immediately communicate with people you are protecting according to a pre-designed approach (part of your security response plan).

3. Update and Optimize Your Video Surveillance System

In an industry where security technology is dynamic and ever evolving, video surveillance systems stand out as the fastest growing segment. It's incumbent upon you and your security partner to be aware of the state-of-the-art solution and the associated benefits.

For example, which would be more helpful?

A) A CCTV system that records individuals walking down a hallway at three in the morning which can only be accessed at a guard desk, or

B) A Smart Video Solution that not only records but also alerts your monitoring station that someone is walking down that hallway, advises them on the action to be taken and allows for easy access to that video on site, off site, on a computer or on a PDA device?

You will want to enlist the help of your security partner to understand and ensure you are using all features of your surveillance system or adopting the correct technology to help you better secure your environment. You should work toward a goal whereby:

- **Your video surveillance system is IP enabled.** Through the use of Internet protocols, your video system no longer needs to be constrained to only one desk in your office. Instead, video can be remotely viewed, analyzed and shared readily with first responders. If any incident points to the benefit of this, Discovery Communications is an example of why this is critical.

- **Your video surveillance system incorporates analytic technologies**. Think of a camera that has the intelligence to analyze what is going on in a scene according to your security policies. If a security breach occurs, your monitoring partner knows it immediately. For instance, if a suspicious object was left behind in your lobby, a smart solution would automatically detect the incident and response would begin right away. A genuine problem experienced throughout the industry is the fact that people watching video get desensitized to what they are looking at and can miss detecting an important security event. In fact, a study conducted by Security Solutions magazine says that after 22 minutes of continuous video watching, a guard will miss up to 95% of screen activity. That's where technology and remote monitoring can close a large security gap.

- **Your video surveillance system is proactively monitored so that it becomes a more powerful deterrent.** A smart system can detect a security breach such as when people are loitering in a loading dock area after hours. The latest industry solutions can then open an audio communications channel via that camera and interrogate or announce themselves to those suspicious people. When using state of the art technology in the right manner, you will gain the advantage of greater deterrence.

4. Become Educated on New Systems or System Designs

There are fundamental technologies in use today that may be new to you.

> The use of visitor management systems can create an acceptable layer of defense, and can even serve to make processing approved visitors more efficient. A new strict employee check-in process is already in consideration by Discovery Communications.
> Turnstiles, in concert with visitor management systems, take that up another level of sophistication.
> IP platforms afford you new flexibility to share data among your team, among your designated responders and with our police and fire departments.

While environments vary, it's important that everyone be educated on options available to them and that you collaborate with your security partner to determine the best design for you.

Your Role and the Role of Your Security Partner

Your role, the role of security technology and the role of your security partner to help you deter, detect and respond to emergencies cannot be understated in mitigating the risk of an attack within the confines of a commercial office building.

A hostage event or siege, although uncommon, can stretch the police to their limits of resourcefulness in attempting to resolve the situation without bloodshed as in the Discovery Communications hostage event. In the Discovery Communications instance, security response plans, building occupant notification and video surveillance contributed to helping resolve the threat. A central part of the resolution involved the Montgomery County Police Department being able to continuously monitor and assess the behavior of the gunman. Through this surreptitious surveillance, the Montgomery tactical officer was able to observe the behavior that warranted taking the shot that killed the gunman and freed the hostages unharmed.

Douglas K. Beaver is an internationally recognized security expert. Doug works for Kastle Systems advising clients on security best practices based on his extensive experience working for Fortune 1000 companies, commercial real estate owners and property management firms, here and abroad. Previously, Doug was the President/CEO of a prominent Washington, D.C. based security organization and senior level executive for a prominent global risk management firm. Mr. Beaver has over 25 years of experience within law enforcement and security industries, and he has provided security consultation, risk assessment analysis and training and on a wide variety of security matters. Mr. Beaver's broad international security experience has taken him to many high threat regions in the Middle East, South America and Asia, where he has provided his security expertise and solution-based consultation. Mr. Beaver is ASIS International Board Certified as a *Certified Protection Professional* (CPP), and he has attained senior level certifications in Homeland Security through the American College of Forensics Examiners. Mr. Beaver has written numerous articles and white papers and has developed enterprise wide corporate and operational security strategies.