Determining Appropriate Protection for Critical Commercial Infrastructure

by David R. Duda, Associate Partner, Newcomb & Boyd Special Technologies Group*

When one thinks of critical infrastructures, some come quickly to mind: the water system, the power grid, the Internet, dams, bridges, roads, air and rail transportation to name a few. Commercial buildings may not occur to the average individual as critical infrastructure, but they are considered as such by the Department of Homeland Security (DHS) and ASIS International. If we think about the impact of the 9/11 attack on the Twin Towers, we understand why. The attack on the Twin Towers cost nearly 2600 people their lives, and launched the United States into a long term war on terror that has increased the national debt approximately 1.5 trillion dollars.[1]

ASIS International's 2011 Critical Infrastructure Resource Guide[2] lists public assembly, sports leagues, gaming, lodging, outdoor events, entertainment and media, real estate (office buildings, mixed use facilities, apartments, etc.), and retail in the commercial facilities sector. Of course not all commercial buildings are "critical" infrastructure. The loss of a storage facility may have little impact on the owner and no impact on the economy or nation as a whole. This means we must evaluate the critical nature of our commercial infrastructure to determine what security or countermeasure we should implement to protect it. This is the purpose of a security risk assessment.

The Security Risk Assessment

Several well established risk assessment methodologies are available, but in essence, to determine a risk level, most rate the assets (people and property) or infrastructure in terms of its critical nature (impact of a loss); threats in terms of their severity and credibility; and vulnerabilities in terms of their exposure. We then concentrate our efforts on mitigating or reducing the higher risks by reducing or eliminating vulnerabilities. In most cases we cannot affect the critical nature of the assets, or the severity of the threats. We can only reduce vulnerabilities.

A typical security risk assessment will use the company's historical data and current intelligence to determine the design basis threats for the development of the risk matrix. These may include:

- Vandalism of property.
- Theft of property.
- Unarmed attack (use of fist or brute force of a nature insufficient to cause death).
- Armed attack.
- Propelled or thrown explosives (rocket propelled grenade, Molotov cocktail, etc.).
- Hand delivered explosives (package bombs or placed bombs) attacks.
- Vehicular delivered explosives (vehicle bomb) attacks.
- Chemical, biological, or radiological (CBR) attacks.
- Cyber-attacks.

Each of these design basis threats will be evaluated against each asset considering various factors to determine vulnerabilities to the threat. A commercial facility that houses a work force of 5,000 will generally require more security than one that houses 5 people. Exceptions can be found in government or military facilities (as the nuclear silo that houses 2 men and weapons that can extinguish the lives of hundreds of thousands, if not millions), but it is generally true in commercial facilities. Likewise, a company that is considered an

(Continued on Page 6)

[1] Kimberly Amadeo, "How the 9/11 Attacks Still Affect the Economy Today," *About.com*, October 22, 2013, http://useconomy.about.com/od/Financial-Crisis/f/911-Attacks-Economic-Impact.htm.

[2] Critical Infrastructure Working Group (CIWG), *Critical Infrastructure Resource Guide 2011*, (ASIS International, 2011), https://www.asisonline.org/ASIS-Store/Products/Pages/Critical-Infrastructure-Resource-Guide-2011.aspx?cart=5c010ddef61943ef8287634d665d443b.

(Continued from Page 5)

icon of the American way of life may make a more attractive target than one that is not a household name.

By examining various "what if" scenarios for each risk, countermeasures are theoretically applied, and the process repeated, to evaluate the proposed countermeasures. A comprehensive security program is then developed around the most effective countermeasures to include the appropriate physical security components, policies and procedures, and staffing and training.

Figure 1 - Arlen Specter Headquarters and EOC, Centers for Disease Control and Prevention, Atlanta, Georgia

Figure 2 - Cobb Energy Performing Arts Centre, Atlanta, Georgia

Risk Mitigation - The Security Program

A comprehensive security program that balances the use of protection resources (people, physical security systems, and policy and procedures) is generally the most effective. A weakness in any one of these components can negate the effectiveness of the other two. Perhaps the best illustration of this is that the best locks are useless if we don't remember to lock the doors.

Low Risk Security Facilities

Physical security for low risk commercial facilities may include a basic burglar alarm system, a few cameras, and the use of good lighting. Security policies and

(Continued on Page 7)

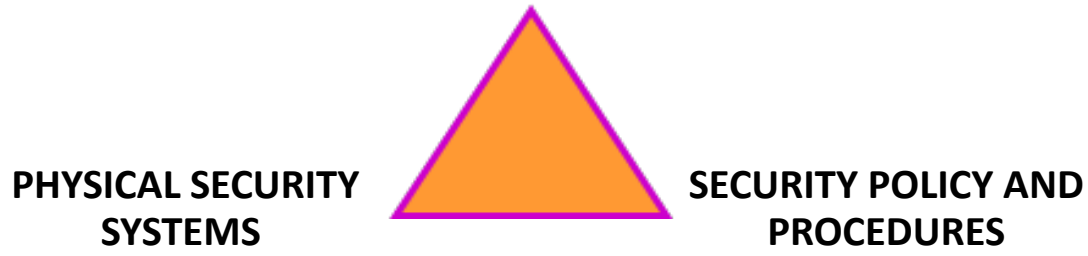

Figure 3 - The Three Components of a Comprehensive Security Program

(Continued from Page 6)

procedures may include those that address disaster management and emergency response (evacuation or shelter-in-place), key control and accountability, opening and closing procedures, video management, pre-employment screening (background checks), prohibited items and substances, drug and alcohol use, and termination. There may be no dedicated security staff, or a few contracted security officers. Security functions may be performed by personnel with other duties. Training may include fire drills and safety and security awareness. The risk assessment will determine the extent to which facilities such as retail buildings, apartment complexes, condominiums, and self-storage facilities will fall into this category. Some of these may not fall into the realm of "critical" commercial infrastructure.

Medium Risk Commercial Facilities

Medium risk facilities may also have card reader controlled access, a computer based visitor management system, intercom systems and/or emergency call stations, and an expanded video surveillance system. Additional policies and procedures may be needed to address security responsibility and accountability, access control (who gets a badge, who gets access to what, who authorizes badges, etc.), workplace violence prevention and intervention (including bomb threats and active shooters), use of archived video, and security post orders, general orders, and special orders. Security staff may include contracted or proprietary security officers. Additional training may be needed for proprietary security staff. The risk assessment will determine the extent to which facilities such as office buildings, conference centers, mixed use facilities, hotels, and retail centers will fall into this category.

(Continued on Page 8)

Figure 4 - Navy Federal Credit Union, Pensacola, Florida

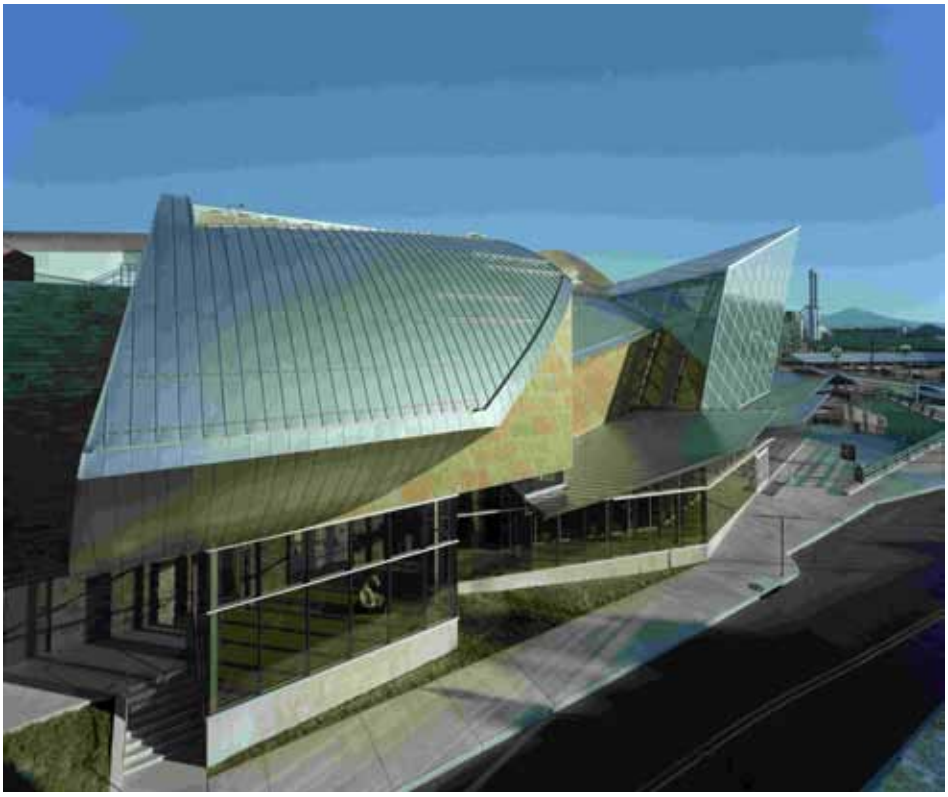

Figure 5 – Taubman Museum of Art, Roanoke, Virginia

The Trend to More Video

Much of the commercial sector is trending towards more video cameras and the use of higher resolution megapixel cameras. Two and five megapixel cameras have become very popular. It is not uncommon for a large commercial facility to have hundreds of video cameras covering vehicle entrances, parking lots, building entrances, emergency exits, loading docks, and infrastructure that is critical to the operations of that facility (such as data centers, server rooms, electrical switchgear, generators, and uninterruptible power supplies).

It is difficult, if not impossible, for an operator to watch a multitude of video camera displays and main-

(Continued on Page 9)

(Continued from Page 7)

High Risk Commercial Facilities

A high risk facility may also have vehicle stand-off enforced with crash-rated barriers (both fixed in place and operable), facility hardening for ram, blast, and ballistic resistance, and X-ray screening systems and magnetometers. Additional policies and procedures may be needed to address occupational safety and health; personal use of company assets; property control, marking, and disposal; and information handling (disclosure, marking, storage, disposal, and destruction). The risk assessment will determine the extent to which facilities such as stadiums, museums, convention centers, casinos, and central banks will fall into this category.

Figure 6 - Taubman Museum of Art, Roanoke, Virginia

(Continued from Page 8)

tain vigilance. Mental fatigue and boredom will set in and the operator will miss important events. This makes it imperative to automate the video surveillance system such that selected monitors only display video when triggered by potential alarm events. This can be done by connecting alarm outputs from the security management system to the video management system and configuring the system such that various events (such as door forced, door propped open, and emergency exit used) cause the video covering the event to be displayed on the alarm monitors. Built-in motion detection can also be used, but is limited to interior locations due to potential nuisance alarms.

Not all cameras cover areas where such alarm triggers exist. For example, a camera covering a fence line does not have any type of switch to act as a trigger. In this case there are special intelligent video analytics software and hardware systems that can provide detection of unwanted behavior, and alert the operator while initiating recording of the scene in question. Some of the behaviors that can be analyzed include:

1. Directional line crossing: virtual line crossing (tripwire) for human and vehicular movement.

2. Movement-in-zone: detection of human or vehicular movement in secure zones where no movement is expected, with filters for direction of movement.

3. Suspicious (abandoned) objects: detection of abandoned objects in an area of interest with filters for size and length of time object is present.

Figure 7 - BlueCross BlueShield of Tennessee, Chattanooga, Tennessee

4. Loitering: detection of person sojourning within a defined zone for a user-defined period of time.

5. Tailgating: detection of person or vehicle crossing a line within a user defined time interval after another person or vehicle. This can be integrated with access control systems.

6. Crowd size detection: alarm generated upon crowd size reaching a user-defined threshold.

7. Moving water vessel: detection of water vessel movement, filtering out waves, sun reflections, and typical waterscape phenomena.

8. Illegally-parked (stopped) vehicles: detection of vehicles stopped in one or more no stopping zones beyond a configurable time threshold.

9. Object removal: detection of object removal from a customer-defined region in a video camera's field of view.

10. Asset protection: detection of the removal of up to 20 objects from a camera's field of view. The event is reported when an object is removed or hidden for more than the specified amount of time.

11. Two-man rule alerts: detection if less than 2 people are present at any time.

(Continued on Page 10)

(Continued from Page 9)

12. Fallen person (slip and fall): detection within seconds of transition from a person's vertical position to horizontal/angled position.

It should be noted that no single video analytics system provides all of the above mentioned capabilities. Additionally, they are more often than not licensed on a "per behavior-per camera" basis and can be expensive to deploy on a wide scale. Therefore they are implemented for specific cameras (such as the camera covering the perimeter fence) and for specific behaviors (such as directional line crossing or trip wire). It is anticipated that the use of these analytics will continue to grow as more become aware of their capabilities and as costs decrease.

Conclusion

Many commercial facilities are considered an important part of the national critical infrastructure. Additionally, these facilities have infrastructure that are critical to the mission of the facility. Just how critical and to what level each should be protected is determined by a security risk assessment. Once the risks are evaluated, various countermeasures or mitigation means are applied and the risk re-evaluated. This process is repeated until effective mitigation measures are determined. Commercial facility owners and operators can find assistance through professional security consultants, the Department of Homeland Security, and ASIS International. The International Association of Professional Security Consultants members provide independent objective security advice on a range of specialties. DHS offers assistance to private sectors through many avenues; one is the DHS Private Sector Resources Catalog. A similar resource offered by ASIS International is the Critical Infrastructure Resource Guide, published by ASIS International's Critical Infrastructure Working Group.❖

**Mr. Duda is an associate partner with Newcomb & Boyd Special Technologies Group (http://security.newcomb-boyd.com). In his 29 years with the firm, he has provided security consulting and engineering services for their various clients, including Fortune 500 companies, colleges and universities, hospital systems, U.S. Government agencies, United States Armed Forces, and state and local municipalities. He served in ASIS International's Critical Infrastructure Working Group in 2012 and 2013.*