WIVENHOE MANAGEMENT GROUP

ONE PHEASANT RUN * MILLSTONE TOWNSHIP, NEW JERSEY 08510-1709
TEL: 609-208-0112 * FAX: 609-208-1295

EMAIL: info@wivenhoegroup.com
Website: www.wivenhoegroup.com

WHAT IS AN ADEQUATE LEVEL OF SECURITY?

Introduction:

Time and time again, the question arises "what is adequate security" for an entity, whether it be a residential hi-rise property, a hospital, an industrial facility, the local energy or water utility, an office building, a college campus, or a school district to name but a few. A number of security professionals will also use the phrase "an adequate level of protection."

The answer is to say the least problematic for the majority of business executives, local government officials, school board members, utility administration management, property managers, and others, as inevitably the decision is based on cost versus safety and liability.

A myriad of factors play into the equation that determines an adequate level of protection for the specific entity involved, which may include one or all of the following major headings:

- **Basis of Security Understanding & Level of Protection**
- **Threat Level**
- **Accepted Security Industry Standards and Practices**
- **Legal Compliance**
- **Environment**
- **Incident History**
- **Liability**
- **Type of Facility**
- **Cost**
- **Risk Acceptance**
- **Insurance Requirements**
- **SVA (Security Vulnerability Assessment) Recommendations**
- **Other**

The list can seem endless, but at the very least, the level of protection for a given entity, regardless of what that entity is, has to be an adequate level that will protect and keep safe the persons and assets from obvious threats as determined by the Threat Level analysis.

1). Basis of Security Understanding & Level of Protection:

There are two definitions of security protection widely practiced in the security industry:

A. **Deter, Detect, Delay & Respond**
B. **Detect, Delay & Respond**

A. Deter, Detect, Delay & Respond:

Many practitioners in the security industry believe that the most effective and cost-effective method of securing a facility is to ideally, **Deter** potential adversaries from breaking into the property by having a clearly defined secure perimeter that will deter any adversary from entering, based on the perceived level of security observed.

Most criminals and even a majority of terrorists are not looking to be caught, or identified and if a particular perimeter protecting a facility appears to be well constructed and more than adequately secure via obvious security systems such as intrusion detection and camera surveillance, they will typically move onto a less secure and protected property.

Remember that a majority of criminals, particularly professional ones, will reconnoiter a facility and study visible security systems, as well as the normal operation of physical security personnel.

An essential requirement for any secured perimeter is to be able to **Detect** adversaries, given that they have not been deterred by specific perimeter security measures. Any security violation or incident can only be responded to if the security breach has been detected. Detection can be via a number of avenues such as an electronic fence intrusion system, exterior electronic intrusion systems, video motion detection systems, ground sensors, video analytic detection and a host of others.

It should also be noted that under the CFATS (Chemical Facility Anti-Terrorist Standards) regulations, the Department of Homeland Security place a high priority on having an acceptable security perimeter that will also detect any intruder that elects to break-in to that facility. Those Standards of Performance are considered to be leading methods of securing and protecting any given facility.

The **Delay** aspect relates to providing layers of security that will delay an adversary, once they have breached the perimeter sufficiently long enough for local law enforcement to **Respond** to the intrusion and neutralize the situation.

In practice, delaying an intruder long enough for local police to respond appropriately is more easily said than achieved. This is particularly true where a facility is located in a remote area and it will take an appreciable time for the police to respond, or where the adversary is a more serious intruder such as a state sponsored terrorist intent on achieving their mission.

True delay is normally only achieved via a “hardened” facility environment, but the cost of installing hardened security measures and infrastructure is at a substantial cost.

B. Detect, Delay & Respond

This basis of security is more generally associated with that required by Sandia National Laboratory, a part of the U.S. Energy Department under their RAM (Risk Assessment Methodology) where there is no acceptance of the **Deterrent** approach and all security is based on having a significant perimeter that will **Detect** an intruder immediately, thus triggering a **Response** initiative and further requiring adequate security measures in place, including “hardening” that will **Delay** the adversary long enough for local law enforcement to arrive and deal with the situation.

It should be noted that the **RAM** SVA methodology was originally developed for the purpose on securing Nuclear Power Plants, but is considered overkill in terms of required security measures for a more normal facility be it industrial, commercial, college, school district, water utility, or other form of entity. As a result, following the **RAM** approach of Detect, Delay & Respond is simply too costly, and in many cases, impractical from an operations point of view to be implemented.

On the basis that **Deter, Detect, Delay & Respond** is the basis of security for a majority of facilities, answering the question of "what is adequate security" for a particular facility, the process will involve studying the following factors:

2). Threat Level:

A major determination of adequate security is conducting a Threat Analysis to establish the credible threat level for a facility, or in simple terms, what is the facility protecting itself from. Over the years, it is astonishing, the number of facilities that have taken security measures without knowing what a credible threat level is for the facility.

The difference is protecting a facility from an extreme threat such as state sponsored terrorist or domestic terrorist is very significant in protecting a facility from theft, or an intruder looking for opportunity, etc.

Determining a credible threat level will involve studying crime statistics for the area, such as found in a CAP Risk Report based on reported crimes accumulated by the FBI via their Federal Database. The categories of crime include the following:

- **Homicide**
- **Rape**
- **Robbery**
- **Aggravated Assault**
- **Crimes Against Persons**
- **Burglary**
- **Larceny**
- **Motor Vehicle Theft**
- **Crimes Against Property**

In addition, assessing a threat level will also take into account local police crime statistics for the same area. The higher the crime rate, particularly in certain categories of crime, the more likely there will be a need for a higher level of protection.

Given a particular facility, a threat assessment will also take into account information gleaned from interviews with local police and residents, often more informative than data produced in local crime statistics. There are many other factors that constitute a true Threat Assessment, not least of which is experience on the part of the assessor, and it is recommended that the threat assessment be conducted by an industry professional with considerable experience and expertise in this field.

Knowing the credible **Threat Level** is fundamental to establishing an adequate level of security.

3). Accepted Security Industry Standards & Practices

As with any industry, there are accepted standards and practices that separate a good security system, including physical security measures, proper installation and training, correct cabling, equipment, and monitoring, etc., and those systems that are based on the presumptions of untrained security installers, least cost equipment, and very often questionable "sales talk" from a security contractor.

Good security systems should be based on sound and specific design criteria related to a particular facility, where the type of security device (camera, electronic access reader, motion detector, alarm point, etc.,) and their location is defined by a clear need for security at that point. Unfortunately, having security design criteria as the basis of implementing security systems is often overlooked, or simply not known.

In the event of an incident and resulting law suit, the first question that arises from the plaintiff's legal team is "what was the design criteria for the security systems and measures," and "why was there no camera or controlled access at the location where the incident took place?" If there is no answer to that question, the facility is already in trouble.

Other standards and practices may also include:

- **Properly maintained equipment and systems**
- **Up-to-date Firmware and Software**
- **Adequate training of security staff**
- **Manufacturer authorized installers**
- **Proper lighting**
- **Accepted system design for particular applications**
- **Training Manuals and Videos**
- **As Built Drawings for all systems**
- **Adequate response time in the event of a system failure**
- **Back-up power systems**
- **Meeting Federal and Local Codes**
- **Minimum video recording time (30 days minimum)**
- **Schedules identifying types and quantities of security panels**
- **Due diligence related to the security contractor**
- **Clear definition of performance requirements of the system(s)**
- **Required installation permits**
- **Electric surge protection**

Even where a facility may be using their own staff to install a security system, it is strongly recommended to have a security professional involved in the supervision and oversight of all installation work and to comment on chosen systems and equipment. This is particularly important where the award of a security system is based on the lowest bid, as opposed to the lowest qualified bid. Security systems may involve life and death situations and should be treated accordingly.

4). Legal Compliance:

With respect to the U.S. and following the tragic events of "9/11," a variety of new security legislation has been passed requiring compliance with the respective rules and regulations that govern such legislation. Security legislation since 2002 includes:

- **2002 – Wastewater Security Act (not promulgated)**
- **2003 – 2004 Public Health Security and Bioterrorism Preparedness and Response Act (BPRA)**
    - **Amended CWA, Required SVAs and Emergency Response Plans for Existing Plants**
    - **Also mandated Procedures to Ensure Food and Drug Safety**
    - **BPRA was a Snapshot – New Facilities Are Not Affected, No Ongoing Review Required**
- **2003 – Hazardous Materials Transportation – 49 CFR Parts 171 – 178**
- **2003 – 2004 Maritime Transportation Security Act**
- **2003 – International Air Transportation Administration (IATA) Regulations**
- **2004 – 2006 City of Baltimore; MD State; New Jersey, New York – various state and local regulations**
- **2006 – DHS Chemical Facility Anti-Terrorism (CFAT) Standards, (ANPR) - 6 CFR Part 27**
- **2006 – Transportation Security Administration (TSA) Rail Transportation Security (ANPR) – 49 CFR Parts 1520 & 1580**
- **2007 – DHS CFAT Interim Final Regulations Rule Effective June 8, and "Chemicals of Interest" List – Proposed**

Transportation Sector

- **Six Distinct Modes of Transportation:**
- **Air: 450 Commercial; 19,000 Regional Airfields**
- **Highway: 4 M Miles of Roads and Infrastructure**
- **Maritime: 41,300 Vessels; 655 B ton-miles Commerce**
- **Rail: 193,000 Miles of Track; 1.4 M Freight Cars; 8 Class I and 550 Other Rail Companies**
- **Mass Transit: 6 K Public Transport Systems; 21 B Passenger Miles/yr**
- **Pipeline: Oil – 177,000 miles; 623 B ton-miles; Natural Gas – 1.3 M Miles of Pipeline**

Air

- **International Air Transport Association (IATA) Section 1.6**
- **49 CFR Parts 1500 – 1550**
- **Effective August 19, 2003 – Air Security transferred to DHS from DOT**

Highway

- **49 CFR Parts 172, 173 Hazardous Materials Transportation**
- **Security Plans**
- **Security Training for Sites with Security Plans**
- **Security Awareness Training for Others**

Hazmat Transportation Security Rule Overviews

•Requirements May Apply To:

•Any person who offers a HAZMAT for transportation in commerce
• Transfer of control of HAZMAT to a person who physically transports HAZMAT off facility's property.
• Any person who transports a HAZMAT in commerce
• Physical relocation of a HAZMAT from the offering facility to an offsite location.
• Minimize HAZMAT transportation risk and liability
• Agency authority to inspect and assess fines immediately following compliance deadlines
• Security Plan must address HAZMAT transportation risks associated with:
• Personnel security
• Unauthorized access
• En-route security
• Security Plan Training
• Security Awareness Training

Security Training

• "In-depth" Security Plan Training, con't
• Frequency
- Initially - within 90 days of Hazmat duties
- "Immediately" following any non-administrative amendment to the Security Plan
- DOT – every 36 months
- IATA – every 24 months
- IMDG – every 3 months (drills)
- Rail – under development
• General Awareness Training, con't
• Frequency
- Initially - within 90 days of Hazmat duties
- DOT – every 36 months
- IATA – every 24 months
- IMDG – quarterly or upon USCG notification
- Rail – under development

Recordkeeping

• Security Plan
• Audit reports
• Training records
- Employee's name;
- Most recent training completion date;
- Description, copy, or location of training materials;
- Name and address of person providing the training; and
- Certification that employee has been trained and tested
- Retain for as long as employee is employed as a Hazmat transportation employee and for 90 days thereafter

Maritime

Maritime Transportation Security Act (MTSA) of 2002

- **U .S. Coast Guard responsible for 33 CFR Parts 101-106, Ports and Waterways Security**
- **Part 104 - Vessel Security Plans**
- **Part 105 – Facility Security Plans**
- **Part 106 – Outer Continental Shelf Facilities and Production Platforms**

Transportation Worker Identification (TWIC)

- **DHS nationally-mandated credentialing program for regulated facilities and operations**
- **750,000 workers will need TWIC certification by September 30, 2008**
- **TWIC security background checks for all applicants**
- **All employees and unescorted visitors will have to apply for a TWIC**
- **125 Enrollment Centers in 38 states**

Rail

- **Rail Transportation Security Act**
- **Proposed Rule, 21 Dec 2006**
- **49 CFR Parts 1520 and 1580**
- **Applies to both freight & passenger rail**
- **Part 1520 – Information Security - rail audits, route information is Sensitive Security Information (SSI)**
- **Part 1580 – Rail Transportation Security – Appoint Rail Security Coordinator, report security concerns to TSA, provide location information to TSA upon request**

Pipelines

- **Transportation Security Improvement Act of 2005**
- **Under the direction of TSA for security, DOT Office of Pipeline Safety (OPS) for safety**
- **Rules are still under development; no specific security requirements or timetable are in place**
- **TSA is developing security standards**
- **OPS conducts inspections, investigates incidents**

- **2008 – DHS CFAT Final Regulations Final "Chemicals of Interest" List Approved**
- **2009 Drinking Water System Security Act (HR-3258)**
- **2010 - 2013 Data Security**

In addition to all of the above, there are now many Data Security & Cyber Security Acts in force, or pending that effectively cover a very large number of industries and entities.

- **NEW AREAS OF INTEREST**
  - **Food Manufacturing**
  - **Education**
  - **Water/Wastewater**
  - **Financial Data**
  - **Energy**

Failure to comply with one or more of the regulations referred to above can result in substantial fines, and in the case of **CFATS** for chemical facilities, can even result in closure of the facility until such time as compliance has been accepted.

Unfortunately, there are a variety of ways to circumvent regulations which will also affect the adequate level of security for a facility. An example is the CFATS regulations requiring several actions if a facility stores or uses a minimum level of various chemicals. A number of facilities reduced their quantities on site of such chemicals, but increased the frequency of deliveries, thereby avoiding the regulations, but increasing the risk occasioned by more frequent deliveries.

There are also many new regulations governing third party security guard personnel. A number of States require security guards to undergo guard training before they are then considered qualified to carry-out security guard duties.

Certain communities require specific buildings based on size as an example to have a physical guard service on a 24/7 basis. Jersey City in NJ is a good example of this type of regulation. It is important to pay attention to compliance with legislation and specific regulations in determining an adequate level of security.

5). <u>Environment:</u>

Establishing what is an adequate level of security and protection for a facility will also be affected by the environment around the facility and within the facility. Areas of particular interest are as follows:

a). Crime Rates

As already mentioned on Page 3, a high crime rate in the immediate area of the facility will certainly affect the **Threat Level**, but the crime rate in surrounding areas may also affect the perceived environment aspect of the facility.

As an example, an immediate facility area may indicate a low crime level, but the area is between two high crime rate areas. It is very likely that the facility will attract adversaries from both high crime areas who consider the low crime rate facility an opportune target.

b). Type of Crime Category

Based on the composition of the facility, the type of crime category listed in any crime report for the area may substantially affect the facility.
Where the facility has a large number of female employees, as might be the case with a large office complex and where employees are required to park their vehicles within extensive parking lots, a high level of crime in categories such as **Rape**, **Aggravated Assault**, **Crimes against Persons**, may require additional security measures to protect those parking areas. This would be even more necessary during the Winter months when daylight is relatively short.

In the same situation, a high level of **Motor Vehicle Theft** would also lead to additional measures to protect all vehicles.

c). Transportation Hub

Another factor that should be considered with respect to **Environment** is where the facility is located in close proximity to a transportation hub where many major roadways intersect and by so doing, provide a ready means of access to the facility and many escape paths after criminal activity at the plant. This reasoning is often considered by potential intruders intent on burglary, robbery, crimes against persons, crimes against property, as well as motor vehicle theft who are seeking to quickly access the property and even more quickly make their escape.

d). Nearby Targets

In certain circumstances, a facility may be in close proximity to a more major target that might include any of the following:

- **Airport**
- **Sports Complex**
- **Hospital**
- **Shopping Mall**
- **Court House**
- **Military Complex**
- **Power Plant**
- **Research Facility**

Adversary groups such as state sponsored or domestic terrorists, activists of various types, and organized crime may choose to create a diversion by attacking the respective facility, particularly with an active shooter incident that would draw local and federal law enforcement away from a major target sufficiently far enough away.

An attack on the other major target would then be more vulnerable with many resources having been diverted to the facility.

e). Sensitive Border

In this situation, the facility borders some form of priority target, and is used as a "stepping stone" to gain access to the target. Possible targets that might border the perimeter of a given facility could include any of the following possibilities:

Main Water Feed for a Community
Main Fuel Feed for a nearby Airport
Sensitive Research Center
Dangerous Chemical Facility
Financial Storage Facility
Datacenter Hub or Internet Main Link
Main Natural Gas Line

From experience, the likely list of "border" targets is both extensive and in many cases, unusual and unexpected.

f). Target Vantage Point

A further environment possibility is that the facility provides a perfect vantage point to launch some form of attack on a nearby entity. In the CFATS DHS Standards of Performance relating to possible threats, security measures are required to counter possible situations involving terrorist groups armed with weapons that include RPG and a variety of missile projectiles.

The intended target could be the immediate landing or take-off flight path for commercial aircraft, or heavy traffic on a nearby highway, or major transportation infrastructure such as a bridge or elevated section of roadway, etc.

6). Incident History:

Determining adequate security for a facility or entity will include looking through incident reports for a period (a typical timeframe would be five years) to assess what type of incidents have taken place during that time and how frequently.

Where there have been incidents such as motor vehicle theft or break-ins to employee vehicles in the parking lot area, this may signal a need for greater perimeter control and surveillance, and perhaps vehicle control systems such as automated gate entry and egress.

Reported incidents involving assault on employees, possible sabotage within the facility, or deliberate damage to equipment including proprietary data may signal a need for a variety of controls involving electronic access control, enhanced camera surveillance, together with increased physical security interaction.

7). Liability:

The shadow of liability law suits pervades every entity, particularly so in the U.S. where any security incident or breach, almost inevitably results in legal action. The repercussions are even more severe if a case of negligent liability, or gross negligent liability is proven.

Hence, it is vital to ensure that any new or upgraded security system and measures address possible liability on the part of the facility. An accepted method of avoiding liability is to carry-out a Security Vulnerability Assessment (SVA) under the supervision of experienced and qualified security professionals.

An SVA is described in greater detail under (10) of this paper, but one result of such a study will be to identify critical assets, as well as the credible risk to the facility.

An SVA will also highlight all vulnerabilities and adversary scenarios, which in turn, identifies necessary Security Design Criteria. This becomes the basis for what security elements will then be required to provide an adequate level of protection for the facility and its most critical assets including employees and visitors.

Failure to address Liability can lead to allegations of negligence as the cause of a security breach, and recent incidents have also resulted in allegations of wrongful death both to the owners and individuals. Even without a guilty verdict in court resulting in substantial punitive damages, the cost of successfully defending a facility against such charges will involve large financial outlay to the legal industry.

8). Type of Facility:

A further factor to be considered in determining what is adequate security is the type of facility. A chemical plant producing highly dangerous products such as chlorine gas, oleum, sulfuric acid and many other types of potentially catastrophic substances, if accidentally or deliberately released, will require a significantly higher level of protection than an innocent office block.

Colleges and schools are considered more vulnerable in today's violent times than a mundane industrial factory producing a product that is not considered of strategic value, or considered a critical element that cannot be replaced easily for other processes.

Another factor is the age of the property. There are many examples of aging infrastructure in a number of industries that constitute critical assets, such as pump stations at water facilities. It would be relatively easy to demolish these buildings by simply driving a heavy vehicle into the infrastructure, thereby putting the pump station out of action for a considerable time and as a result, leaving a community without drinking water and a water source to fight fires.

Other factors could include mandatory public access making it more difficult to maintain a true perimeter; whether it is an animal research facility that might attract attention from animal rights activists; is it a storage facility handling valuable items such as gold bullion, rare works of art, sensitive and highly confidential data where security would be at a higher level; the building has irreplaceable historic value and other factors.

Any of the factors mentioned above would affect the necessary level of protection required.

9). Cost:

Many would insist that cost is the leading factor in defining what security is possible for a given facility. However, cost is also a "double-edged sword" in that the cost of not providing adequate security could be many times greater than any single security system cost.

A current security situation involves a property being sued for wrongful death and negligent liability for failing to provide adequate security, and in particular, failing to provide a security guard during the period 8:00 AM to 4:00 PM. A tenant was killed by an intruder entering the building (following other tenants into the building, as there was mechanical access control in operation). In an unusual move (most lawsuits of this type are settled "out of court"), the case is going to court as the plaintiff refuses to settle for less than $30 million.

The cost of security can also be affected by how a security contract is awarded. In quite a number of bid situations, the contract is awarded to the lowest bidder, but this can prove very expensive later if the bidder is unable to provide the new security system for the price they bid. Many bidders will deliberately tender a very low bid figure, anticipating that they will be able to claim a substantial number of change orders during the contract installation period.

If the client did not use a security consultant to design the new system, or was unclear in the RFP documentation, allowing the contractor to claim any number of problems that were not covered specifically, the ultimate cost of the contract can be two or three times the original low bid figure.

A professional security analysis that then provides the basis of design for the necessary security will avoid a multitude of change orders, and will also provide a point of responsibility for the furnishing of the system. Clients who simply call in three or more security contractors to propose new security for a facility often don't realize that in the event of an incident caused by an alleged failure of security, the liability and responsibility for security remains with the client as the contractor was only trying to provide what the client requested.

Over the last year or so, there has been a series of technology and installation developments that will significantly reduce security costs. These include:

- **Cloud Memory Usage**
- **Wireless Networks**
- **Remote Monitoring**
- **Smart Communications**
- **Internet Access**
- **Enterprise Security System Sharing**

10. Risk Acceptance:

One of the interesting features of a full-fledged Sandia National Laboratory RAM (Risk Assessment Methodology) SVA is that the result provides an actual calculation of a facility's risk level. However, the risk level can be modified by changing numerous parameters to arrive at a different level of risk. This can be higher or lower. In short, a facility management can decide the level of risk that they are prepared to live with.

Unfortunately, this is a "double-edged sword" as many executive suites are prepared to accept higher risk in favor of lower security cost, forgetting that, in the event of a serious security incident, the liability level will almost certainly jump to Negligent Liability, as they chose higher risk in an effort to reduce cost.

In a court of law, that is a recipe for disaster in the form of punitive damages. However, understanding different levels of risk including mitigation, and utilizing experienced security professional advice may be appropriate in a number of cases, but caution should be exercised, and relying on contractor or manufacturer salespeople is not recommended without serious investigation and demonstrated results.

11. Insurance Requirements:

The insurance industry, driven in part by the escalating cost of medical expenses and increasing values of critical assets, together with the ever present threat of terrorism that exists in the world today, looks on security in a different light within the business community.

As many will be aware, insurance companies have for many years insisted on U.L. Certified Alarm systems for applications involving the Banking, Jewelry, High Value Retail industries, and others where insurance companies are being asked to insure high value items against theft. In today's world of cyber crime, terrorism, negligent liability and a host of other adverse factors, insurance companies are also requesting in a number of situations, a qualified SVA (Security Vulnerability Assessment) report and proof that the entity in question is following a program of security improvements recommended in such a report.

Conversely, companies who can demonstrate that they have carried-out such assessments with experienced and qualified security professionals then certifying the results, can expect, and should demand a reduction in their insurance rates.

12. SVA Recommendations:

As already mentioned earlier, the majority of new security legislation requires that an entity carry-out a Security Vulnerability Assessment (SVA). The methodology may vary by industry, but essentially an SVA provides the following:

A). Correct Threat Level Identification:

It is particularly important in any security environment to know the level of **Threat** that a facility or organization is facing before considering the various improved security options available, or in simple terms the who or what, that the facility should be protecting against.

There is a significant difference, both financially and manpower-wise between protecting facilities from a State Sponsored Terrorist Group as opposed to dealing with theft, or other form of criminal act, or a disgruntled employee intent on making a statement against their employers.

B). What To Protect Most (Critical Assets):

As with (1) above, it is also important to identify those **Critical Assets** that must be protected at all costs (those assets that if compromised, are likely to have the most serious consequences for the organization), given that it is not possible to protect everything.

It is unfortunately true that 100% protection of all assets is extremely difficult to achieve for both financial and logistical reasons. Correctly identifying the Threat Level and Critical Assets are essential to then determining Security Design Criteria.

C). Security Design Criteria:

As already stated above, there is no such thing as guaranteed 100 percent security (the ingenuity of the human mind precludes such a goal), and thus it is vitally important to have **Security Design Criteria** (those specific reasons as to why a certain security system was installed in place of another, and why security devices such as cameras and access control readers were placed at certain locations and not at other points within a facility).

A professional SVA will identify such Security Design Criteria, and allow an entity to defend itself against alleged wrongdoing in the event of an incident. Applying correct design criteria will also, in a majority of cases, avoid unnecessary cost brought about by implementing security systems that are either "overkill," incorrect for the proposed purpose, or addressing aspects of security that are trivial in nature with costly measures and equipment.

Many clients do not have design criteria of any sort for their facility, and in the event of an incident and court action, one of the first questions asked by the plaintiff's attorneys is "what were the design criteria for the installed security systems?" The inability to answer this question immediately places the defendant in a less than favorable light.

D). Findings & Recommendations:

Perhaps the most important section of an SVA, as this section provides an invaluable assessment of those issues most likely to have serious consequences for the organization.

A professional assessment of such issues is generally based on both many years of security industry experience, where the consultant team has experienced first hand, what should be in place in terms of security measures, and what is effective and what is not. The same assessment is also likely to be based on direct experience with current legislation, and knowledge of pending legislation.

Recommendations will also illustrate cost/effective and reasonable methods of addressing such issues, while limiting the security solutions to those necessary to meet specific requirements and/or legislation. Again, a professional SVA prevents "overkill" and excessive cost in dealing with security issues.

E). Federal Grant Funding:

There is considerable Federal Grant Funding available at this time, both from Stimulus funding, and from a variety of other Federal and State funding programs that can be used to offset the cost of any required security improvements, etc.

These grants can cover many different areas ranging from training grants, and information technology to advanced electronic security systems that include communications, security management, CCTV Camera Surveillance systems, vehicle control, and others.

Recent examples are Federal grants given to companies located from the Brooklyn Navy Yard, NY, to facilities on a major waterfront area in Illinois, where the grants ranged in value from $150,000 to $1.5 Million and above.

A professional SVA is often the single most important document supporting such Grant Applications.

F). Customer Confidence:

Many commercial organizations have utilized an SVA as a means of increasing their customer's confidence in their ability to provide reliable and protected services and/or product.

By instituting an SVA and then commencing an appropriate implementation program concerning the agreed recommendations of the SVA, the organization has then communicated such actions to their customers as further reason for the customer to have the utmost confidence in their chosen supplier of goods and services.

Fortune 1000 companies in particular, are primarily concerned about the reliability and continued capability of suppliers to continue to provide goods and services in the event of an emergency.

In a municipal environment, it is particularly important for the community served by that organization to have faith and confidence in the provision of expected services, especially during an emergency situation.

Loss of Public Confidence with a municipal group or department can have very serious consequences, and is a major terrorist goal.

G). Counter Liability:

In the event of an incident within an organization or at a facility, the event would almost certainly be followed by a lawsuit that is also likely to allege some degree of **Negligence** or even **Gross Negligence**. The inability of the organization or facility to demonstrate that they had already carried-out an SVA by a qualified party is likely to be seen as an immediate example of the failing of that entity.

Note: It should be remembered that the implementation of SVA recommendations is not governed by a precise time period, and from experience, many recommendations can be implemented using existing manpower with minimal cost. Thus, it will be exceptionally difficult for any defense team to prove any form of negligence where an SVA was performed, and where at least a part of the implementation program is shown to have been underway.

An SVA specifically addresses situations which may be considered liable for the client.

H). Development of a Phased Solution:

An SVA provides an opportunity for a client to address potential security problems in a flexible manner, and over a phased implementation period. In many cases, it is possible to develop a phased timetable of implementation based on asset protection priority, and over several years.

It also allows a client to incorporate security requirements, whatever they might be, and whether it is to meet legislation or prevent possible liability, over a period of years, thus easing the financial strain of having to meet security requirements in a hurry following an incident, etc.

I). Emergency Planning & Preparedness:

One of the byproducts of a professional SVA is typically the updating of any Emergency Response Plan, not to mention the correct identification of critical assets within an organization or facility.

Knowing the full extent of potential consequences of given actions, an organization is thus able to better respond to an emergency with appropriate resources at minimal cost, and to be able to demonstrate their overall preparedness for such emergencies.

J). Measured Response:

Where an SVA has identified correctly, the credible Threat Level, and Critical Assets, and likely consequences of criminal, terrorist, or negative insider actions, an organization or facility can deploy the appropriate resources to address a situation.

From experience, the measured response is likely to be far more effective, and also likely to be more cost-effective taking into account the findings and recommendations of an SVA than it would be without the benefit of such information.

SUMMARY:

Once the basis of security understanding has been selected, being:

Deter, Detect, Delay & Respond (an approach practiced by a majority of Professionals in the security industry)

or

Detect, Delay & Respond (an approach recommended by Sandia National Laboratory in their RAM Series of Security Vulnerability Assessments)

There are many factors that will determine the adequate level of security and protection for a facility that include:

- **Threat Level**
- **Accepted Security Industry Standards and Practices**
- **Legal Compliance**
- **Environment**
- **Incident History**
- **Liability**
- **Type of Facility**
- **Cost**

SUMMARY (Continued):

- **Risk Acceptance**
- **Insurance Requirements**
- **SVA (Security Vulnerability Assessment) Recommendations**

It should be noted that a professional SVA, in essence covers all of the above factors and the recommendations of such a report will outline the necessary and what would be considered an adequate level of security and protection for a specific facility.

The more important factors are Threat Level, Legal Compliance, Type of Facility and Liability.

A threat analysis is important in identifying what the facility is attempting to protect itself against. Likewise, it is also important to ensure that the facility is in compliance with all applicable security legislation, both current and pending.

The type of facility (high risk or aging infrastructure) will play a key role in determining an adequate level of security and protection, as will the identifying of critical assets, the most important of which is human life.

Last but not least, the level of security and protection should also ensure that there are no gaps in security that could lead to negligent liability in the event of an incident.

The author of this paper is David McCann, principal consultant with Wivenhoe Management Group, who will be happy to answer questions and address comments. He can be reached at dmccann@wivenhoegroup.com.

Wivenhoe Management Group **March 2014**