# 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

## TWELVE IMPORTANT POINTS TO CONSIDER WHEN REVIEWING SECURITY SYSTEMS IN TODAY'S ENVIRONMENT

**Introduction:**

Security in all its facets is an on-going process and any new or upgraded security system should be audited on a regular basis. However, many organizations and companies "rush" into security changes without considering these twelve important considerations.

**1). What is the Credible Threat Level?**

Before an organization begins to invest in upgraded or new security measures, shouldn't they know what it is they have to protect against? Threat levels can range from **Simple Graffiti** to **International Terrorism**. For most companies and organizations, it will be in a range from **Insider or Outsider Theft** to possible **Violence in the Workplace**.

The difference in cost and manpower however, can be very significant. Before a company begins to invest in security systems, it is well worth the time and effort to identify the Threat Level.

**2). What are the Critical Assets?**

Identifying critical assets is essential for one major reason. It is an accepted fact in the security industry that it is not possible for both cost and logistical reasons, to protect everything. Thus, a key issue is identifying those assets that if compromised, would do very serious damage to the operation of the entity. These assets vary from company to company, but typically can be people, inventory, infrastructure, process, data, patents, equipment, public confidence and others.

Good security will have identified those assets and apportioned funds and resources based on critical assets priority.

**3). Are there Compliance Requirements?**

Many industries such as Transportation, Healthcare, Chemical, Education, and Water and Wastewater are now required to meet existing or pending new **Security Regulations** such as **CFATS, HIPPA, BPRA, 49 CFR, MTSA** to name a few with significant penalties for non-compliance.

Any new security measures should ensure compliance with both current and pending security legislation and operational requirements.

**4). Is the Company Correctly Addressing its Liability?**

Liability involving any form of security incident is costly, even where an entity is defending what appears to be a strong case. Legal costs are not inexpensive. Far worse are situations where a company may be at fault and is facing a "negligence" situation and is thus facing substantial damages.

These situations can be avoided by executing a Security Vulnerability Assessment (SVA), which is normally the first stage of most security legislation now in force. Utilizing a specific SVA methodology, or simply "best practices for the industry" will identify potential liability situations, including security systems that do not operate correctly, do not meet an adequate level of protection, or were an "after-thought," and were not professionally planned with gaps in security as a result.

It is believed by many security professionals and by the politicians that write legislation, that virtually all companies of substance will be required to carry-out an approved SVA.

**5). Has the Company Adequately Identified Key Design Criteria for its Planned Security Measures?**

In the event of a security incident and subsequent legal action alleging failure of one or more security systems, one question from the legal team of the plaintiff will be "What Design Criteria did the company use for their security measures and systems?" Failure to produce same will immediately place that company in a difficult position and imply that there was negligence.

Design criteria constitute the reasoning for the design and placement of security systems and security devices. Examples include the reasoning for positioning a camera in one location over another, or why certain doors were controlled and others were not.

A well-executed SVA will provide design criteria as part of the recommendations.

**6). Are the New Security Measures Up-To-Date and Easily Upgraded to Meet Future or Additional Threats?**

New or upgraded security systems, and particularly integrated security systems are not inexpensive.

It is important to avoid obsolete technology and to ensure that whatever equipment and systems are chosen, that they are up-to-date and can be easily upgraded later to reflect changes to the facility, or to the threat level.

Very often, security systems are implemented without adequate planning and for the lowest possible price. Security technology, like all technology, changes rapidly and implementing a security system that cannot be easily expanded or modified to accept new technology can prove to be a rather costly later when changes are required.

## 7). Who is Responsible for Security?

A senior manager should be responsible for overall security, but it is also important to have a "hands-on" middle manager responsible for day-to-day operation of the security department, whether large or small. This person would also be responsible for preparing incident reports and following-up incidents.

From experience, the quickest way to have a security system taken for granted and for the original intent to disappear, is to have no one in charge at a senior level.

## 8). Emergency Response

When an incident occurs, it can be a serious crime, and may even be a life threatening situation. Security systems are only as good as the people monitoring and operating the system. With an increasing number of incidents involving violence in the workplace and even "shooter" events, it is necessary to have an Emergency Response Plan.

The emergency response plan is a "living" document indicating what actions should be taken in any given emergency. Live rehearsals of this plan should be mandatory and reasonably frequent. There is nothing worse than having an emergency incident and then finding that the emergency response plan manual is missing and that staff are confused and panic stricken due to a lack of knowledge and live training.

## 9). Are the New Security Measures Practical?

Any new or updated security system must be practical in terms of the work environment. Again from experience, many security systems fail because they did not take account of work routines and industrial processes.

If the only way that an industrial operation or process can take place is to temporarily deactivate the security system, such as allowing certain doors or entry points to be uncontrolled, it will not be long before that becomes the norm.

A security system must be practical to the point that associated and affected staff "buy-in" to the system, realizing that it is in their best interest and safety to do so.

**10). Training**

Many new security systems are implemented and system training is an hour or so of training by the security contractor installation staff that installed the system. No new security system should be activated unless at least two members of staff are able to operate the system, understand all reports and screen displays and are able to quickly operate and do basic programming on electronic access control computers, as well as camera surveillance digital recorders or control computer head end equipment.

Ideally, there should not only be adequate instruction material, whether electronic or hard copy, but there should also be an instruction video that instructs authorized staff to view step-by-step, how to perform all essential actions required by the system.

**11). Security Audits**

Any new security system, even when designed by professionals against strict design criteria and SVA results is based on a "snapshot in time," that window when the security system was put together. Facilities and companies change due to growth, changing environment, new regulations, etc. It is therefore important to carry-out security audits, perhaps once a year where the security system and measures are tested for compliance and whether they meet current requirements.

**12). Second Opinion**

Prior to moving ahead with the implementation of new security measures and systems, particularly where significant funds are involved, it is recommended that the company or entity have an experienced security professional study the proposed equipment and system operation and give a qualified opinion on the capability of the system against what the entity believes the system will do.

The cost of such advice is usually very reasonable and in terms of preventing what may be a major mistake by the company, also invaluable.

**TWELVE IMPORTANT POINTS TO CONSIDER WHEN REVIEWING SECURITY SYSTEMS IN TODAY'S ENVIRONMENT**

**Note:**

**The twelve points are stated in a succinct manner, but arriving at answers as to whether a company, facility, organization, or entity has adequately addressed each item may require significant effort and expertise.**

**While a company may elect to carry-out such research and assessment internally, it is strongly recommended that an experienced security professional be involved, if only to study the approach and subsequently look over the results.**

**Wivenhoe Management Group** **January 22, 2013**