SECURITY ASSESSMENT

You can't know where you are going, if you don't know where you have been. Secondly, the security remedies of today differ significantly from the remedies available five or ten years ago. The good news is that as technology has evolved, costs have gone down. *For example, consider the cost of a video surveillance system 15 years ago compared to today.* There has be a gradual shift from reliance on security personnel to the application of many new and divergent technologies. Twenty years ago, infant abductions were a clear and present danger. The NCMEC were regularly reporting infant abductions. As new technology evolved, infant abductions were brought under control.

The security officer of today has the potential to be the glue that synergizes the effectiveness of a wide range of security technologies. There have also been substantial decisions as to how to best leverage security assets in a manner that ensures that the whole is greater than the sum of the parts.

There have also been significant shifts in the ambient threat environment. These shifts have had an impact in the defining of a reasonable standard of care. More and more, the standard of care is being shaped by tort law. Security driven litigation, the case-law that has evolved. In turn it has impacted the totality of security planning. A significant amount of security consideration, during the planning phase, is driven by the desire to avoid the liability claim, of inadequate security. The dilemma for hospitals is the desire to project a welcoming environment, while at the same time, providing adequate security and safety for patients, visitors and staff.

The goal of ensuring that each security program meets the reasonable standard of criteria, should not be the only driving force behind a security program. Loss prevention is not solely about liability. Loss prevention is also applicable to the security of plant and equipment, as well as inventories and supplies, as well as proprietary information.

Security Management Services International

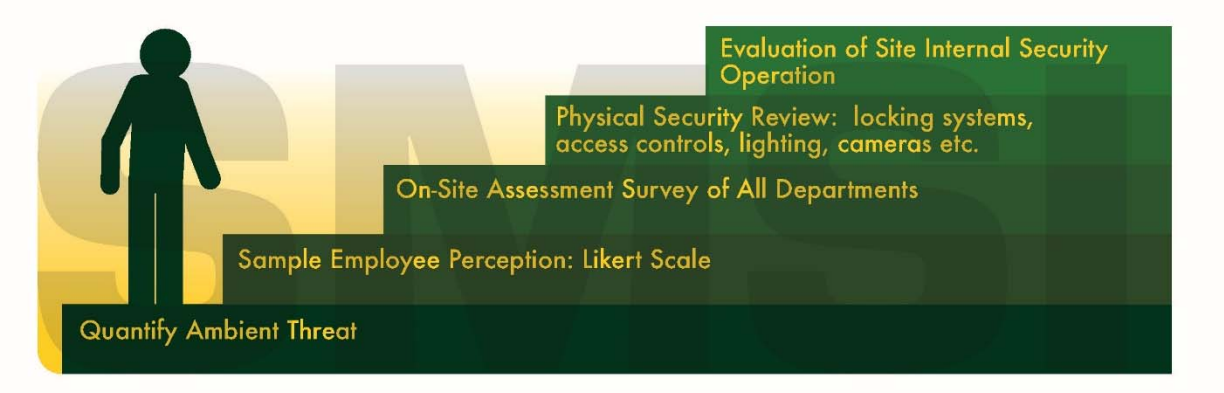
SMSI, Inc. • 1168 Pan Court • Newbury Park, CA 91320 P 805.499.3800 E bill@smsiinc.com

Therefore, the application of security technology and security personnel must be driven by quantifiable need. Do not make the mistake of assuming the mere existence of security technology, such as video surveillance systems, will deter criminality.

SMSI Inc. is a security consulting firm that specializes in the assessment of the security and loss prevention needs of hospitals. Our team brings a wealth of *hospital security expertise* to the table from both the private and public-sector perspectives. Furthermore, SMSI has no conflicts of interest, in that we are not engaged in the provision of guard services and/or the sales of security systems (video, lighting, access control, etc.). Therefore, the SMSI team brings objectivity to our mission by addressing the unique and special needs and interests of each of our clients in the determination of vulnerabilities and the subsequent recommendation of solutions. Bear in mind that the cost of reaction almost always exceeds the cost of being proactive. Unlike the universal precaution practices of hospitals, security is very much a situational discipline.

SMSI has substantial experience as forensic security experts in cases that claim inadequate hospital security operations, usually in the wake of an alleged security breach. SMSI understand how to reasonably mitigate most claims of negligence. We also understand the need to mitgate intentional tort claims, such as the excessive use force or false imprisonment. Over the last 25+ years workplace violence cases have included homicides, infant abductions, parking lot attacks, sexual assault cases, and active shooter cases. Hospital security programs must be pre-emptive, supporting the goals of deterrence and prevention. This requires reasonable anticipation. Hospital security programs are usually held to the *highest standard of care*. Reaction, after the fact, is far more costly than prudent prevention.

Consider this fact: According to the most recent issue of the Journal of Healthcare Risk Management, of the 12 defined Sentinel Events, five have security implications. Additionally, a recent poll found that 68% of Nurses have experienced at least one incident of violence, while 20% have experienced nine or more. Rarely a week goes by without a newsworthy report of a serious security breach of a hospital, with workplace violence leading the way.



Given the assumption that security is a situational discipline, we offer the above construct as a guideline to the progression of our security assessment process. The first step requires defining of the ambient threat environment, using the CAP Index and other available data, such as police crime data, as well as internal incident data. Without this data, the security program may be predicated on mythology. Second, the success of every security program is a direct function of employee buy-in. With this objective in mind, we have created a

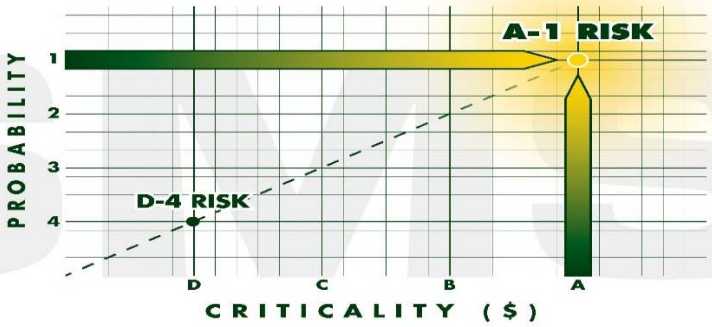
Likert Scale to measure employee's perception regarding safety and security. We want employees to know that their opinions are important.

The SMSI assessment process leaves no stone unturned. This includes the evaluation of the efficacy of physical security methodologies presently in place, such as locking systems, surveillance systems, access control systems (including visitor control) and CPTED design (steps 3 & 4). Finally, the security organizational structure will be evaluated for both effectiveness and efficiency. Under the best of circumstances, the security organization must be the glue that gives the entirety of the security program quantifiable success (step 5).

As qualified Security Expert Witnesses, having dealt with numerous cases wherein there has been assertions of inadequate security, we have found, that in most cases, that the presence of inadequate security, would have been discovered within the context of our security review. The cost of Prevention, is almost always more cost-efficient than reaction, after the fact. Moreover, security reviews are generally very cost beneficial in that they introduce the application of new security technology, which in almost every case, reduces cost by moving from manpower to emerging technology. Security programs must also be pragmatic and reasonable, to be accepted.

As previously noted, a unique methodology of our security assessment process, is that we encourage the input of every employee. Employee perceptions are important to eventual success. Therefore, with anonymity, employees are requested to respond to our online, to the **SMSI Likert Questionnaire** (as noted in step 2 of the assessment model). This proprietary questionnaire samples employee perceptions as relates to their perception of the security program. We have noted that employees who participate in this aspect of the assessment process, are much more likely buy into the resultant solutions.
Our team is also uniquely conversant with the techniques and sensibility of **CPTED** (*Crime Prevention through Environmental Design*) principles. Three of our team members are **Certified CPTED Practitioners**. *These qualifications are generally unique.* As security and loss prevention consultants, our mission is the reasonable mitigation of preventable security breaches that affect patients, staff, guests, as well as property. Within our assessment process, we rely on direct observations, as well as quantifiable hard data.

The model below depicts **SMSI's two-dimensional analytical process**. This model quantifies security risks from the perspectives of both probability of occurrence and the financial criticality impact of occurrence.



VULNERABILITY ASSESSMENT MATRIX

As part of the evaluation process, the **SMSI Vulnerability Assessment Matrix** provides both a quantitative proportional and budgetary paradigm for the application of reasonable and actionable corrective remedies.

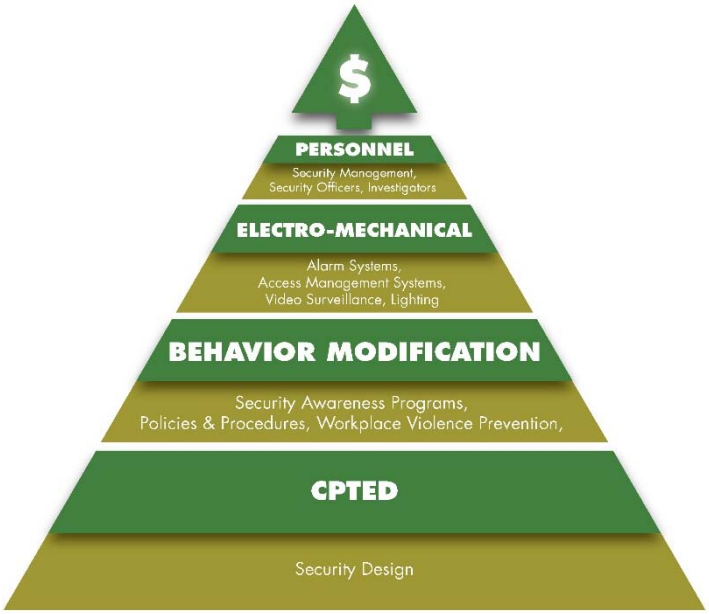
Security Management Services International

SMSI, Inc. • 1168 Pan Court • Newbury Park, CA 91320 P 805.499.3800 E bill@smsiinc.com

This model considers the probability of occurrence and the potential resultant cost of inaction. This means that a D-4 risk (low probability of occurrence, low financial impact) would likely by mitigated by low cost procedural remedies. On the other hand, a A-1 Risk will almost always require a budgetary response.

Consequently, the Matrix above helps to model the budgetary process as well as providing a paradigm of *reasonable deliverables, thereby* ensuring that our remedies are need-based. There is also the need to satisfy accreditation agencies, such as JCAHO, OSHA and various state and federal agencies. However, the mere compliance with regulatory guidelines and standards, does not necessarily mitgate liability.

Clearly the cost of Prevention is almost always more cost-efficient that reaction after the fact. When the assessment process has been completed, our mission is to then turns to the determination and prioritization of reasonable, and acceptable, corrective actions. Our security solutions model is situationally effective and budget priority sensitive. The **Security Solution Hierarchy, *using Maslow's Hierarchy of Needs*** *as a model*, provides a roadmap for a hierarchal security program, by applying less costly remedies, before the application of the costliest remedy, *Security Personnel*.



SMSI, Inc.
SECURITY SOLUTION HIERARCHY

Consistent with our previous models, you will note that the **Security Solution Hierarchy** applies the least costly remedies first, with subsequent remedies to follow when needs justify.

The **SSH** assures effective implementation of *need-driven security remedies*, thereby ensuring optimal return on investment**.** *The Security Solution Hierarchy provides a cost-effective construct, and a hierarchical model for any credible hospital security program.* The Hierarchy also factors into the process the *accumulative positive impact* of a wide range of security methodologies, thereby enhancing ROI. The foundational construct of CPTED provides added value and effectiveness to all hospital security programs by reinforcing the concept of unity of purpose. CPTED implicitly encourages the notion that every employee has a role in maintaining effective security. *The mitigation of a single WPV incident will most likely cost-justify the entire security assessment process.*

Collectively, the SMSI Inc. Team offers the following qualifications:

- The SMSI team has more than 35 years of hospital security and loss prevention experience.
- We have been retained in hundreds of security litigations as forensic expert witnesses covering over 30 states, and Puerto Rico. (These cases have included, but are not limited to: infant obductions, sexual assaults, battery, excessive use of force by security personnel and aides, and substandard security design.

Security Management Services International

SMSI, Inc. • 1168 Pan Court • Newbury Park, CA 91320 P 805.499.3800 E bill@smsiinc.com

- The SMSI Team includes former law enforcement officers.
- We have also worked cases involving inadequate background checking, and/or credential verification.
- We maintain memberships in ASIS International, ASHRM, SCAHRM, ACHE, IAHSS, ICA & Cal DOCA Certifications: CPP (Certified Protection Professional); CMAS (Certified Master Anti-Terrorism Specialist); CHEPS; PSM (Physical Security Manager); CHPA (Certified Healthcare Protection Administrator); CFE (Certified Fraud Examiner) & Certified CPTED Practitioners.
- Certifications: CPP (Certified Protection Professional); CMAS (Certified Master Anti-Terrorism Specialist); CHEPS; PSM (Physical Security Manager); CHPA (Certified Healthcare Protection Administrator); CFE (Certified Fraud Examiner) & Certified CPTED Practitioners.

It is important to reinforce the notion that CPTED is a very cost-effective security strategy. Three of our team members are Certified CPTED Practitioners.

Consider the following questions:

- Has your hospital conducted a comprehensive security review in the last 3 years?
- Does your hospital presently rely on Site Specific CrimeCast Data?
- Is your security program overly labor intensive?
- Is your security program optimizing cost-efficient current security technology?
    - Is your video surveillance system an asset or liability?
- Has every hospital employee participated in security awareness training program based on ambient need?
- Are employees trained to recognize the incipient signs of potential work place violence?
- Have you evaluated the pros and cons of contract security officers versus a proprietary security force?
- Is security the technology (video, locking and access control systems) over 5 years old?
- Has your security design maximized the cost-effective strategy of CPTED (both interiors & exteriors)?
- Is the security department using security management software?
- Are security decisions data driven?
- Have your security officers been certified for the hospital environment?
- Is public access control to your hospital commensurate with a reasonable standard of care?
- Does your background checking vendor ensure no negligent hires?

CPTED FOR HOSPITALS

SMSI also offers a wide range of optional Security Management Support Services. Visit our **LinkedIn Group: *Security Source Online***. We welcome the opportunity to submit a comprehensive security assessment proposal specific to the needs of your hospital. If you would like to receive further information, do not hesitate to contact me. ***As an aside SMSI*** *also offers separate and distinct onsite,* ***Workplace Violence Mitigation Training****, customized to your hospital's specific needs. This program would be helpful to the security management team, the risk management team, human resources and the employee health management team This onsite*

Security Management Services International

SMSI, Inc. • 1168 Pan Court • Newbury Park, CA 91320 P 805.499.3800 E bill@smsiinc.com

workshop also recognizes the mitigation role of each employee. The most effective security results from total employee involvement. This includes the ability to recognize the potential threat at the incipient stage of aggression cycle, when intervention is most successful. We would be happy to provide further information on this topic, in the form of a special proposal. The goal is to involve employees as part of the solution. Therefore, every employee should understand the principal that: **If You See Something; Do Something.**

Appropriate training will answer the questions: See What, and Do what?

The optimal opportunity for **Crime Prevention Through Environmental Design** is preconstruction. However, it may be effectively applied to the built environment. This cost-effective strategy will, pay dividends and can become the glue that holds the entire security program together, and it will contribute to the reduction of premises liability claims in most cases. It was not our intention to overplay CPTED, but the cost benefit of this strategy is substail.

The essence of the services we offer herein, reflects our ability to understand your specific the specific security needs, as well as the means, by which, to address those needs. The value of this offering, is illustrated in our five-step assessment approach presented herein. In the wake of our assessment process, we also offer the option of ongoing *security management support services*, including the protection of your interests in dealings with security vendors.

With minimal amount of proper training, all employees can, and should become informed observers of the signs of WPV at the incipient stage. Those employees can be empowered to recognize potential threat, and to initiate the process of mitigation. This training is also appropriate for contracted employees such as greeters, housekeepers and facility employees. The mitigation of threats is very successful, when those threats are recognized, and mitigated, in the incipient phase.

Do not hesitate to email or call me with any questions you may have. As security professionals, our mission is to anticipate and to mitigate the threat, including both internal and external acts of dishonesty and criminality. Hospitals, and their patients, visitors and staff all deserve a reasonably safe crime free environment. Good security is simply good business for all hospitals. The most cost-effective conclusion, is to act now, as opposed to reacting later. Upon your request, and a brief conversation, I would be happy to submit a detailed and site-specific proposal. This Proposal address the specific needs and security concerns of your hospital. The Proposal will also include letters of recommendation.

President:

William H. Nesbitt, CPP, Certified CPTED Practitioner
Member: ASIS International; IAHSS, ICA, Cal DOCA, ACHE, ASHRM, SCAHRM