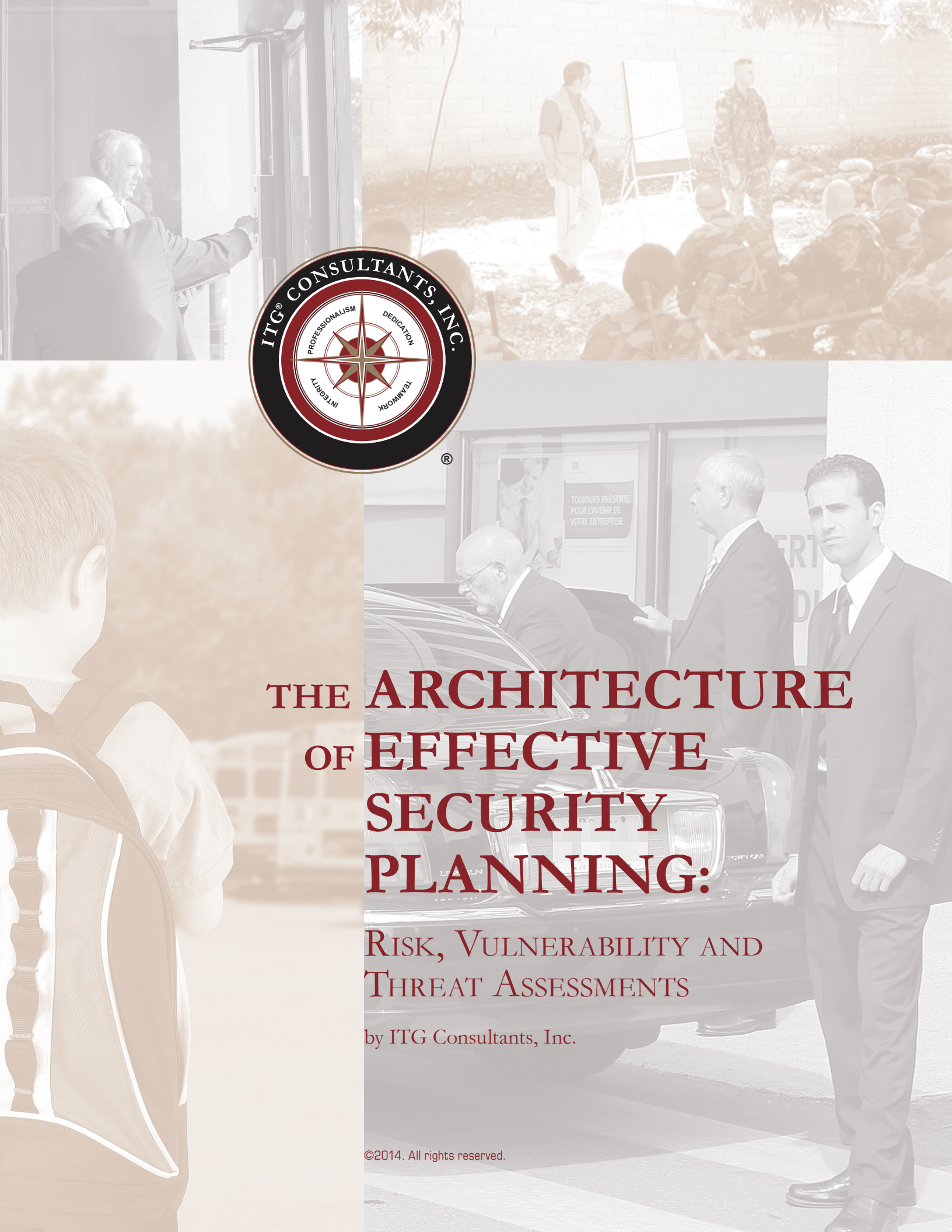


THE ARCHITECTURE OF EFFECTIVE SECURITY PLANNING:

Risk, Vulnerability and Threat Assessments

by ITG Consultants, Inc.

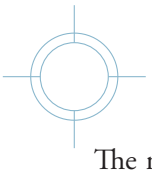
CONTENTS

INTRODUCTION

One crucial mistake too many organizations make—regardless of type or size—is failing to recognize the need for a comprehensive security program. A false belief that negative events are more likely to happen to the "other guy," lulls many into not undertaking this important process. Even those that perceive the immense value of having a program often don't develop plans due to a lack of internal resources or the skills necessary to do so. To confound the problem, the responsibility is often delegated to persons without adequate skills, and the resulting plan is deficient. Adding to the challenge, sometimes the concept of security planning is misunderstood. The term risk management becomes confused as it is commonly used by insurance, financial and security practitioners who seek to reduce risks from differing perspectives. In spite of the complexities, however, there is a way to create a thorough, practical and effective plan that need not be daunting, confusing or exorbitantly costly.

Security planning is a methodical process designed to help organizations identify risks, vulnerabilities and threats to their operations—all of which can negatively impact their ability to achieve their objectives. Understanding the terms of security planning is fundamental to understanding the value and purpose of planning:

- **Risk** Anything that can potentially impact an organization negatively. This includes environmental occurrences such as earthquakes or tornadoes, or man-made ones, as in the case of data theft.
- **Vulnerability** A weakness or inability to withstand the effects of a hostile environment. Includes physical structures (i.e. weak door locks) and technological weaknesses (i.e. inadequate IT firewalls).
- **Threat** A risk (as defined above) that is currently materializing; the impending manifestation of risk in the near-term timeline. A threat causes the most damage to an organization at points of vulnerability, whether through environmental causes or malicious human intent.



Cultivating a culture that values safety and security is a leadership mandate that originates from the mindset that negative events can happen anywhere and to anyone.

The need to engage in this practice of security planning applies to entities of all types and sizes, even those previously thought to be safe havens, such as schools.

Nearly all organizations take steps to protect the electronic data associated with their operations. The security of physical assets and personnel deserves the same, or greater, level of attention. A comprehensive perspective on security will address risk across the full criminal spectrum, from egregious workplace violence to simple theft. Once developed, the plan will account for ways to prevent, mitigate and respond to the identified risks and threats. Recent decline in law enforcement's involvement and response to corporate risks and threats have shifted more responsibility to the organization itself, increasing the necessity of thorough planning. Without planning, when a problem materializes, the staff will be forced to address the situation from a reactive posture, which is inherently subject to countless pitfalls.

MAKE PLANNING A PRIORITY

Planning for security is an essential business practice. The 9/11 Commission Report elevated it to an operational imperative saying, "Preparedness is not a luxury; it is a cost of doing business." A culture of safety and security is dependent on leadership and education.

Leadership

Leaders set the tone for security planning in their organizations. If they demonstrate concern for safety and security, the rest of the entity will follow suit. Conversely, if leaders fail to prioritize planning for such concerns, the result will be an organization ill-equipped to handle any adverse events that arise. Cultivating a culture that values safety and security is a leadership mandate that originates from the mindset that negative events can happen anywhere and to anyone.

Education

Education is an integral piece of effective planning because it fosters buy-in from all parts of the organization. When key stakeholders educate the whole organization in the need for preparedness, the team falls in line to ensure the goal is met. Knowing the implications of being unprepared (liability, loss of life, disrupted operations), engages everyone, from the leader to the lowest man on the totem pole, in the process and increases the odd of achieving the objective.

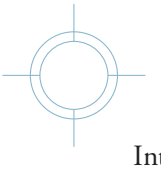
RESPONSIBILITY FOR SECURITY PLANNING

Unless an enterprise has a security-specific position in its organizational structure, in-house personnel are unlikely to have an adequate knowledge base with which to assess all manner of risks, threats and vulnerabilities. Even in instances where security is the sole mandate of an employee's job, having additional expertise from a skilled consultant provides great benefit and allows the employee to stay focused on his primary tasks instead of allocating significant time to the effort of assessment and planning. Enlisting the aid of a security professional is not a mark of incompetency. Quite the contrary, it demonstrates the proverbial wisdom of two heads being better than one.

Unless an enterprise has a security-specific position in its organizational structure, in-house personnel are unlikely to have an adequate knowledge base.

Finding *the* right consultant to weigh in on matters of organizational safety and security is critical. Consider the following items when vetting security professionals:

1. Are they members of the local chapter of the Better Business Bureau? Have any complaints been registered against them?
2. What certifications do they hold and to what professional organizations do they belong?
3. Ask for a list of references and contact them.
4. Does the consultancy firm carry liability insurance? Are they willing to add their clients to their liability policy to cover errors or omissions that may emerge later?
5. How much of the work will have disclaimers applied to it? Is the firm's chief concern protecting themselves from potential lawsuits or helping their clients navigate the security planning process with professional recommendations they can stand behind?
6. Consider the depth and breadth of their experience, not just the number of years in the industry. The application of their trade across multiple venues and circumstances results in broader understanding and acquisition of more skills.
7. Will the consultants facilitate the entire process (assessment, recommendations, implementation and follow-up) or is their service limited to only a portion of the process?
8. Will the consultants assist in vetting, and potentially managing, vendors and integrating components (CCTV and alarm systems) of the larger system to prevent incompatibilities between components (a risk of ad-hoc approach)?
9. Does the consultant have a vested interest in the client's purchase of components or services? Are their recommendations aligned with the client's best interest or potential profit derived from the sale of specific components/services?



Interview more than one consultancy firm in order to develop a thorough understanding of available services and assess degrees of competency.

OTHER CONSIDERATIONS

Undertaking the task of developing a comprehensive safety and security program may seem daunting. Hiring expertise is an effective way to ensure the process is efficient and effective, especially where professional experience is shallow or absent in the existing organization. Bear in mind these additional considerations when determining whether to develop a plan and how to allocate resources toward that effort:

Role of law enforcement

Many organizations subconsciously believe that the security of their personnel, information and physical assets is the responsibility of local law enforcement. While the police (or respondents from a similar jurisdiction) do respond to criminal activity, the organization must provide its own first line of defense against risks, threats and vulnerabilities. Deferring that task to law enforcement is a reactive posture that only addresses the problem after events take place instead of aiming to prevent them from occurring at all.

Policies and procedures

Corporate entities, non-profits and academic institutions are legally obliged to have policies to ensure the safety of their employees and students, in compliance with OSHA and other regulations. Their preparedness for such events may qualify them for better insurance coverage, as well. Similarly, there are laws governing employment policies, such as equal opportunity, and privacy of information. While only a handful of defense and energy companies are subject to federal mandates to have security policies, the failure of companies—no matter their industry—to develop them constitutes a hole in the entity's overall policy governing their operations. Security plans are distinct from each of the previously mentioned policies, but are an integral part over the global operational plans.

Budgetary issues

Obtaining insurance is a cost of doing business in today's litigious society. Any organization that hopes to operate with longevity purchases insurances policies to cover liability in the event of crises taking place. The premiums paid are an investment made to ensure the company's ability to continue operating. Investing in a security program is of commensurate benefit and works similar issues from the preventative side of the equation. Preparedness for security crises sometimes prevents them altogether, but, at a minimum, the effort and cost stems the losses when they do occur.

No organization will thrive without the ability to preserve existing resources.

Conducting assessments and implementing a plan are actually far more cost-effective than acquiring and installing components on an ad-hoc basis. Developing an overall system from a strategic perspective ensures that all the systems work together appropriately. For example, access control systems (card readers, automatic door locks) should communicate with systems recording entry/exit times and activate CCTV cameras to that area. If the components are purchased separately, they may not be compatible, which could require additional investments to modify or replace the items. Furthermore, having a comprehensive perspective on security issues will ensure that no more than what's necessary is purchased, eliminating the cost of unintended redundancies in the system. Additionally, when a full-scale implementation isn't immediately feasible financially, having a comprehensive plan for staged implementation ensures the systems will be forward-compatible and upgradeable at later junctures.

Protecting existing capital assets through security measures is vital to long-term success. No matter how much revenue is generated, an organization will not thrive without the ability to preserve existing resources. This may never be more vital than in the earlier life stages of an organization, when most are tempted to delay the investment in planning for security. The Insurance Information Institute estimates that nearly 40% of small businesses never re-open after a natural or man-made disaster.[1] Professional consultants can also aid in making the case for an investment in security planning, as their expertise can illuminate both the fiscal and legal ramifications of neglecting it.

THE SECURITY PLANNING PROCESS

The initial step in developing a comprehensive security plan is simply to ascribe value to having a plan before a crisis occurs. If an ounce of prevention is worth a pound of cure, the nominal investment made to develop a plan is worth many times its cost in losses averted or reduced. Once the decision to plan has been made, the workflow commences as follows:

1. **Conduct Assessments** Evaluate the need for hiring security expertise to conduct the assessment process based on the knowledge, expertise and tools existing in the current staffing mix. Vet consultancy firms as necessary. Assess the organization's exposure to each of the three categories (risk, vulnerability and threat). The information that comes from these assessments identifies specific issues and provides recommendations to help bolster defenses against them.

[1] *FEMA, Red Cross and Ad Council Launch New Ready Business PSAs to Urge Small Businesses to Prepare in Advance of an Emergency* (accessed March 20, 2014). http://bit.ly/1kYyv2P

2. **Create a Plan** A well-conceived, well-written security plan will include these key steps:
   - Conduct a risk assessment to identify any items that would inhibit their ability to continue operations.
     - Prioritize the findings and recommendations from the risk assessment.
     - Determine timelines for implementing recommendations.
   - Conduct a vulnerability assessment to evaluate exposure to technical, structural, environmental, topographical, and geographical hazards that could adversely impact operations (e.g. IT firewalls, door locks, natural disasters).
     - Prioritize the findings.
     - Develop contingency plans, security policies and enhancement plans to address the findings.
     - Determine timelines for implementing those plans and policies.
   - Appoint a multi-disciplinary threat assessment team (TAT) to evaluate risks that may escalate to threats.
     - Conduct threat assessments as indicated/necessary.
     - Evaluate need for additional expertise according to threats presented (mental health, specialized security, etc.).
     - Develop a Threat Response Matrix (TRM) as a scalable, adaptable contingency plan to guide and assist in responding to potential incidents.

A multi-disciplinary threat assessment team (TAT) is essential in accurately evaluating risks.

- Modify contingency plans from the TRM to address specific threats, as they arise.
- Implement plans; threats are current and demand immediate response.
- Reassess periodically (ongoing until threat dissipates).

3. **Implement the Plan** Once assessments have been done and a plan created, the next step is implementing the recommendations. Time, budgetary considerations and other constraints may limit implementation. Therefore, the findings need to be prioritized to determine which risks will be addressed immediately and which need to be staged over time and fiscal resources. Financial limitations aren't the only reason some recommendations might not be implemented. The culture and purpose of the organization also need to be factored in to the equation. For example, schools wish to retain an environment conducive to learning and may opt not to install metal detectors at building entrances though they would be an effective deterrent against would-be shooters. **If an entity opts out of implementing some of the recommended changes, they need to understand the possible liability considerations associated with that decision and take steps to bolster other defenses to compensate for it.** Of vital importance, however, is ensuring that all the implementations are effective for the goal they are meant to achieve. For example, the mere purchase and installation of closed-circuit television monitors (CCTV) doesn't necessarily mean surveillance will be effective. The monitors must be viewable remotely and fields of view need to be labeled accurately to provide valuable information in a timely fashion during a hostile circumstance.

4. **Evaluate and monitor:** Security plans are dynamic in nature. They cannot be developed and then relegated to a binder on a shelf. Instead, they should be working documents, updated frequently to reflect the changing environment (i.e. political, economical) in which the organization operates. Maintaining a security plan is simpler and less time-consuming than the initial effort of developing one. Active monitoring ensures that maximum benefit is derived from the planning process.

CASE IN POINT

Consider the following cases to aid in understanding the benefit of security planning. Ethical considerations preclude sharing actual client information, however these sample illustrations are typical and provide an excellent frame of reference.

Corporation president's personal residence

A risk assessment identified the possibility that the president's home could be targeted due to his publicly documented income and high-profile role in the company. His residence was subsequently assessed and the following vulnerabilities were identified: (1) He lived in an attractive neighborhood, adjacent to open space and main traffic arteries, making the home easily accessible to perpetrators. (2) The home has a below-grade finished basement with a walkout exit and stairs leading to the ground level. This entry was lit with a single, small porch light, and had no motion detection sensors. The door was glass and could be easily broken to gain entry, though the door was monitored by the alarm system. Recommended implementations (new door, motion sensors) were declined. At a later date, the alarm company notified the homeowner of unauthorized entry to home. (The risk of being targeted had escalated to a threat.) The home was entered through the basement door; theft of personal property occurred.

Had the recommendations been implemented, the threat may have been mitigated or prevented completely. The cost of a solid door and motion sensors to illuminate the basement entry would have been less than the property losses sustained as a result of the burglary.

School campus

A risk assessment was conducted on the school's grounds for preparedness against active shooter scenarios that have increased in recent years. The school had previously acquired a closed-circuit television system in an ad-hoc effort to prepare for such situations. In the course of the vulnerability assessment, the CCTV system was identified as having points of weakness to bolster for defense in a school violence scenario: (1) the cameras were only viewable over the campus Wi-Fi. This made it inaccessible to law enforcement until they were on-site and eliminated the possibility of advance preparation. (2) The camera system was not mapped on a diagram. Nor were the camera angles named in a way that conveyed their locations in the building. This rendered them less effective to law enforcement for their intended purpose of locating a perpetrator within the facility. (3) The camera DVR recording system was enclosed in a protective cage to prevent tampering or disablement, but the cords extended beyond the cage. This

The value of security planning is gauged by the degree of preparedness that results in fewer losses in operations downtime, the ability to respond instead of react, and minimizing the potential impact on lives and livelihood.

allowed for a perpetrator to simply unplug the system entirely, rendering it useless for its expressed purpose. (4) No external command post had been identified for law enforcement to utilize; verification of being within Wi-Fi range to view cameras had not taken place.

Recommendations made were (1) to liaise with local law enforcement to establish a command post location, (2) to determine method for sharing camera viewing with law enforcement, (3) expand DVR cage to protect the cord, (4) re-name cameras and develop map illustrating the camera locations. Each of these implementations bolstered the school's ability to defend against, and effectively respond to, the possibility of an active shooter or other unauthorized personnel, on the campus.

News organization in metropolitan area

As a matter of doing business in the public eye, a news organization began receiving threatening mail, containing powdery substances similar to anthrax, in the wake of 9/11. A risk assessment demonstrated reasonable concern over the likelihood of similar packages being received in the future, and additional risks resulting from co-tenancy with government offices. The vulnerability assessment revealed gaps in their mail-handling systems.

Recommendations made were (1) to limit access to the mailroom to only authorized personnel through installation of an access control system, (2) to establish systems for handling mail to identify suspicious packages before delivery to intended recipients, and (3) to educate recipients on procedures to limit contamination and to decontaminate if exposed. Implementing these systems positioned the organization to handle the existing crises and any future, similar instances that could arise due to the nature of their business.

VALUE

A cost analysis can never be accurately run on an investment in security planning because its value is measured in the events they prevent or mitigate. Only when a crime actually occurs can proof of the investment be established. Even then quantifying the dollars (or lives) spared is impossible. As such, the value of security planning is gauged by the degree of preparedness that results in fewer losses in operations downtime, the ability to respond instead of react, and minimizing the potential impact on lives and livelihood.

CONCLUSION

Having a comprehensive security program is vital to the longevity of every organization. Protecting human lives from harm and safeguarding existing assets are an obligation that can't be dodged for a lack of skill, limited funds, or failing to prioritize them. Enlisting the help of private security consultants ensures that the assessment process is thorough and easily understood. Their professional expertise supplements the existing skills of the organization and facilitates a cost-effective implementation of the recommended steps. No organization should be without an effective security program.

ABOUT ITG CONSULTANTS

ITG Consultants, Inc., is a Veteran-owned small business based in Pennsylvania providing training, consulting and security management services.

David L. Johnson, president of ITG, is certified in Homeland Security – Level V, by the American Board for Certification in Homeland Security, previously served on its Executive Advisory Board and also serves as Chairman of The American Board for Certification in Dignitary and Executive Protection.

Gale R. Ericksen, vice-president of ITG, is a Certified Protection Professional by the American Society of Industrial Security and is certified in Homeland Security – Level III.

Together, the leadership team of ITG Consultants has nearly 6 decades of experience in international law enforcement, executive and dignitary protection and training.

For more information or a no-obligation discussion, visit our website at www.itg4.com or call (866) 904-4ITG.

BBB ACCREDITED BUSINESS

BBB RATING: A+