In an ideal world, our schools, colleges, and universities would be immune from the threats and challenges that affect other businesses and institutions. Unfortunately, we do not live in an ideal world. Academic institutions are cross-sections of society and bear the same responsibilities for the safety and security of their populations and infrastructure. This cross-section brings with it all the problems that affect people away from school with the added factor of being the most vulnerable population in our society. There is a profound moral and legal responsibility to provide a safe and secure environment within which learning can take place, driven by the fact that learning must take place in a sheltered setting and the concept of profound trust awarded to the school administration that the children and adolescents will be protected while under their care.

Like any business, academic institutions have assets that include a diverse cross-section of people, including students, faculty, staff, guests, contractors, community partners, and others. In addition to the human assets of the institution, there are hard and soft assets that are critical to the operation of the organization. Hard assets include buildings, equipment, and supplies; soft assets include reputation, personal information, and research. Each institution has a responsibility to provide a safe and secure environment that encourages and fosters a positive learning experience for its students within a diverse, complex, and dynamic environment and population. This is a daunting task for administrators who address conflicting priorities on a daily basis often with fiscal restraints that can affect decisions.

Unlike a business which leases office space or owns a manufacturing facility, schools – particularly private primary and secondary schools, colleges and universities – are built so that the campus consists of multiple buildings around open spaces, vegetation, and walkways. This design – based on Thomas Jefferson's vision of the "academical village" – is aesthetically pleasing and conducive to the growth and diversity of an academic institution, but it also creates challenges to security.

Good security programs use a cohesive blend of physical security, electronic security, policies and procedures, and security staffing in their facilities to help reduce overall risk. Physical and electronic security measures, when properly utilized, offer great benefits in deterrence, intervention, and investigations. A security threat assessment examines certain aspects of an existing security program and exposes inconspicuous flaws that may not be evident until misfortune strikes.

What is a security threat assessment?

- Security programs are a comprehensive blending of people, processes, and technology that require the allocation of adequate resources.
- Everyone at the school – including students, faculty, staff, and guests – has security responsibilities, but security leadership begins at the top with trustees and administrators.
- Key components of any security program are communication and awareness which begin in the business plan

A security threat assessment is a systematic review or analysis conducted by professional security consultants to examine the effectiveness of current security practices. The assessment identifies security deficiencies and includes a review of all security measures presently in place to determine their effectiveness and functionality as well as their usefulness to the overall security effort. Once the assessment is completed, recommendations are made to correct deficiencies, mitigate security risks, and protect the schools assets. Ideally these recommendations become the road map that school administrators use to develop a security plan as a part of the school's business plan.

The development of a system of safeguards for the protection of assets, visitors, and employees of any specific facility requires identification of vulnerabilities. Although each facility is different, the discipline, planning and careful attention to each detail is the same. The assessment format should include interviews of key personnel, review of the physical facilities, review of applicable policies and procedures, review of the operation of any existing security program and equipment, and site inspections. Assessments should include security vulnerabilities from both outside and inside the organization. The end product of a security threat assessment should include a detailed written report and may include an oral presentation for designated leadership. Report findings should be specific to the organization and should be based on best practices and industry standards

A security threat assessment may be referred to as a *vulnerability analysis*, a *security survey*, a *security threat analysis*, a *security review*, or even a *security audit*. The two terms most consistently used by professional security consultants when referring to a review of the vulnerabilities of an organization or company are *security threat assessment* and *security threat survey*. When using the term *vulnerability assessment*, some people tend to think of safety issues rather that security issues. For the sake of simplicity, this document will use the term *security threat assessment.*

Using employee interviews, physical observations, and the questionnaire results, a consultant will identify potential security threats to the organization, predict their probability, and determine their criticality to the organization should such an event occur. This means that consultants will first use historic data and observations to identify specific threats for which protection may be required. Second, the likelihood of each of those individual threats becoming a reality must be determined. Finally, the resulting effect on people – students, faculty, staff, visitors, and the community – and the school – property, reputation, and operation – must be determined. The risks and recommendations are formulated and are usually prioritized and ranked as to their importance to the organization. Information is compiled in a formal report that is presented to the client after the assessment is completed.

A full security threat assessment is an in-depth study of all risks and threats, both perceived and actual. The assessment covers a wide range of topics to include the physical interior and exterior features of the building or buildings. Entrances and exits, including stairwells, are examined. Doors and windows are evaluated as to physical characteristics and durability. Locks and other security devices are examined for deficiencies. Security policies and procedures, if in place, are reviewed for effectiveness and completeness, and the assessment will determine if employees are complying with the security policies and procedures. The surrounding perimeter – including parking lots, lighting, and vegetation – are all scrutinized to see if they are within security standards. Alarm systems, card access systems, CCTV systems, and all other security devices are assessed to determine their efficiency.

In some security threat analyses, a questionnaire is filled out by a cross-section of the stakeholder population (usually 10 percent). They are asked for their views and feelings on selected security issues. The results of the questionnaire are then analyzed, summarized, and presented in the report.

An assessment may cover all of the vulnerabilities an organization may face or it may be limited in scope to cover a particular need or deficient area. Most assessments are limited in scope and are designed by the consultant along with participation of leadership to meet a particular need of the school or organization. This is often true where there is a precipitating event or mandate that is being addressed. For example, the scope of an assessment may omit computer security, outdoor lighting, policy and procedure, or any number of other areas to reduce the time and expense of the assessment.

Unlike the full security threat assessment, the limited scope security threat assessment only covers certain selected areas or issues. Any part of the complete survey may be omitted for any number of reasons. The assessment may be only for lighting or vegetation or may only cover the current electronic security system. The reasons why organizations opt to use a limited scope security assessment are varied. Some owners or administrative staff are comfortable with much of the security devices and practices already in place, and only want a particular agenda followed that is based on security plans, security needs, or available budget. For whatever reasons, the security threat assessment may be limited to cover only certain areas of risk but still address most of the security risks facing an organization.

The security threat assessment is a document that outlines deficiencies in security procedures. Some corrective actions may take longer than others because of budgeting concerns and the seriousness of the deficiency. Budgeting over a period of years may be needed to correct certain deficiencies.

Many security deficiencies are not as obvious as others. Should an incident result in a civil proceeding against the organization, any other similar incidents in the past may influence a judgment against the organization in civil court. Reactive and pro-active actions taken by the organization prior to the incident may very well save the organization thousands or even millions of dollars in damages. Hiring security professionals to conduct a security survey is a good way to identify and eliminate or mitigate security risks before an incident occurs. A security threat assessment provides an unbiased "snap shot" of the organization's security program and security gaps.

Once the organization is presented with the knowledge of security deficiencies, any failure to take action could be used against them in court during a civil liability proceeding. One of the most serious setbacks an organization may face during a litigious proceeding is the introduction of evidence revealing prior knowledge of an existing condition but a failure to act upon or take steps to alleviate or correct the condition. If the organization has set a goal to correct all deficiencies and is presently working toward completing that goal, the position of the court has usually favored the company. A critical question will be, "Has the organization taken reasonable steps to correct deficiencies?"

A security threat assessment educates and raises security awareness among personnel. In an academic institution, this would include students, faculty, and staff. The assessment points out security deficiencies that may then be corrected. When people know that the organization is concerned about identifying and correcting security deficiencies, there is a general feeling of co-operation and improved morale.

By implementing the recommendations provided in the security threat assessment, the organization will experience a number of benefits. The most important benefit will be a safer environment for all students, staff, faculty, and visitors. A second benefit is the education and enlightenment of all personnel on meeting and maintaining accepted security practices and standards. Finally, liability to the organization is reduced – or in some cases eliminated – when an incident occurs on school property.

How do you choose a security consultant?

Not all security consultants have the necessary background and experience needed to identify risks and recommend changes. Many so-called security consultants are actually salesmen representing their company's products. Be wary of walk-through security surveys that include only a brief report or may even exclude a written report entirely. An important question to ask is, does the firm supply the security equipment or the security personnel that may be recommended, or do they only specify and recommend equipment and personnel? Some firms may be inclined to recommend services and equipment that benefit them as a company, not their client.

There are a number of ways to protect your organization when deciding to hire a security consultant to perform a security assessment of your organization.

- Is the company or individual a member of ASIS (American Society for Industrial Security)?
- Does the person conducting the security survey have the credentials of a CPP (Certified Protection Professional) or PSP (Physical Security Professional)?
- How long has the company conducting the assessment been in business?
- What is the reputation of the security firm?
- What other security threat assessments has the company performed?
- Are previous customers satisfied with their work?

You may want to determine if the security firm designs security systems or provides bases of design. Most security firms will want to conduct their own security survey before providing a basis of design because of liability concerns. If the firm conducting the security survey does not design security systems, much of the work may have to be redone before a final product is ready. Additional expenses may be incurred over and above those already paid.