# NEW STRATEGIES
# FOR
# K-12 SAFETY AND SECURITY

In the aftermath of September 11, 2001, Federal, State and Local authorities all turned their attention to assessing their security posture. Each began making the necessary adjustments to ensure proper levels of security. Educational institutions soon followed in its attempt to improve campus-wide security. However, unlike the many others, educational institutions received no funding support from the new Department of Homeland Security.

Educational institutions are far beyond the list of critical infrastructures outlined by the federal government, but provide an interesting target for terrorist. Recently, people around the world tried to explain the reasoning behind the terrorist attack on a Russian school. To date, no solid conclusion has been made of that attack. However, many security professionals saw such an attack to be consistent with typical terrorist targeted results. The ultimate goal of most terrorist attack is to cause mass terror by inflicting harm on a large number of individuals. Many security professionals see America's educational institutions as a "perfect" target for such mass infliction of harm. Although our educational system may not equate 1-to-1 with others on our Nation's list of critical infrastructures such as our transportation system, power grid, and our financial institutions, it is still believed to be a "successful" target for terrorist.

Against the backdrop of the enormous tragedy at Virginia Tech, colleges and universities nationwide are reviewing emergency preparedness protocols and physical plant security at their institutions. Official reports stated a wide spectrum of failures that ultimately contributed to the catastrophic end-result. Of great importance during this event was the breakdown of both internal and external communications as the events unfolded.

The Pennsylvania Amish School and other recent school shooting caused alarm within the K-12 environment and have alerted school administrators to develop strategies for increasing their security posture. One disadvantage seen within the K-12 environment is its lack of both security professional on staff and its use of outside consultants to help determine vulnerabilities on campus and assistance with developing strategies to reduce and/or eliminate threat. However, K-12 school administrators are recognizing the need for both and many have employed Directors of Security for the school district. Having experience in the industry, many Security Directors are seeking the help of professional security consultants to assist with Security Assessments and District Wide Security Master Planning.

## TARGET REDUCTION STRATEGY

In an effort to reduce the risk of being an open target to terrorist and others seeking to inflict harm on students, faculty and staff, many school districts are beginning to conduct risk analysis and vulnerability assessments of their campuses. Many of them start by conducting market research to determine the right contracting support and associated task

list to be used when conducting a campus or district-wide comprehensive security assessment.

The intent of the security assessment report is to highlight both general and specific findings and briefly describe recommended security improvements required to strengthen each schools security posture. A second goal of the report is to highlight ways of diminishing the district's potential liability exposure.

## THE STARTING POINT

A comprehensive security assessment should include identifying and evaluating the "AS-IS" condition of each school by assessing its physical assets, information technology infrastructure, current video surveillance, access control and intrusion detection technologies and conducting a review of current security policies and procedures. Recommendations should be developed with a strategic understanding of the all on-going capital improvement projects. Considerations for the out-years should be identified as "TO-BE" upgrades and should be incorporated as part of the security assessment report. Recommendations and solutions for modifications and upgrades should be developed with an understanding that all processes, systems, and resources must be integrated to provide a comprehensive campus or district-wide security management plan.

Within the security assessment report, milestones should be identified for an integrated security management system upgrade that is compatible with the District's capital improvement plan and the levels of protection consistent with the protection of students, faculty, staff and other key assets. Vulnerability assessments should include on-site surveys, perimeter vulnerability analysis, access control, security technology evaluation, and security resources and training assessments.

The assessment should address the following task areas:

**Task Area 1 – Policy Analysis and Development:**
Recommend security requirements, policies, procedures and standard operating procedures based on reviews, analysis and assessment.

- *Vulnerability Assessment* – Review, analyze and recommend changes.
- *Evaluation of Countermeasures* – Assess current procedures, techniques and technology. Develop/recommend countermeasures for campus implementation.
- *Continuity of Operations, Contingency and Emergency Response Planning* – Review, analyze, evaluate, and recommend changes.
- *Cost Analysis* – Complete cost/benefit analysis of security technologies and human resource proposed solutions.
- *Security Management* – Perform a professional security review and analysis, and provide recommendations regarding the district's security force and security management needs.

**Task Area 2 – Perimeter Physical Protection:** Addresses physical security and access control as the first line of defense for protecting the campus environment. It includes:

- Perimeter and interior access control (*visitor identification and access control*)
- Traffic and barrier planning
- Parking
- CCTV surveillance
- Metal detection
- Emergency response capabilities
- Intrusion detection

**Task Area 3 — Technology Evaluation & Analysis:** Assist in identifying and recommending security products and applications to upgrade security and surveillance system technologies. Considerations should include:

- Local digital surveillance camera implementation, which may be integrated into a district-wide CCTV surveillance system.
- School emergency communication system, which may consist of the campus-wide public address system, campus radio, and room-to-room paging. A parent notification system should also be considered.
- Access control technologies (card readers, remote entry, etc.) should be assessed to provide visitor control during school hours and to secure any special access areas designated by school administrators.
- An assessment of district-wide intrusion detection systems should be conducted in an effort to protect school technology and other assets. Also an evaluation should be done of the current maintenance contract strategies district-wide.

## SECURITY METHODOLOGY FOR CAPITAL IMPROVEMENT PROGRAM

There are two cost effective and efficient ways of integrating a safety and security program within a district-wide capital improvement program.

1. Mandate all security requirements to be a part of the Architectural Design and Review Process as it is with the fire, public address, audio visual and Internet systems. By doing so, the responsibility of selecting a security consultant to provide digital surveillance and other security requirements would lie in the hands of the Architect Firm.
2. Each capital improvement program is typically managed by a construction management and consulting firm. Just by the nature of its independence from others involved in the project and its loyalty to the end-user, this would be a perfect place to solicit additional consulting support. The teaming of construction and security consulting firms is often done as a measure to eliminate additional contract vehicles and because the construction management firm is generally responsible for all aspect of the capital improvement program.

## FINDING PROFESSIONAL'S SUPPORT

The first step in selecting a security consultant or consulting firm should be to verify its true independence of manufacturers and system integrators. The benefit in doing so is to ensure the consultant is working on behalf of the school district and is not there to deliver any preconceive solution. Remember, the selected security professional could be a part of your in-house staff. In-house security professionals may also provide a non-bias and independent view of your security needs.

The next step is to verify company or consultant's credentials with respect to the specified task areas. The qualified company or team should have security professionals with associated professional certifications. The company or consultant should also possess senior level engineering and/or project management skills. Physical security professionals will typically have the following certifications:

- Certified Physical Security Professional (PSP)
- Certified Protection Professional (CPP)
- Certified in Homeland Security (CHS)

Remember, professional experience may be more important than credentials and those with experience can bring to bear industry's best practices.

The contractor should also provide a project manager for the security assessment task. This individual should have:

- Proven experience in managing security programs and conducting analysis, studies, and assessments.
- Proven capability working in security management with threat analysis and vulnerability assessment experience.
- Demonstrated experience as a security consultant developing security programs, integrating security systems and products and managing federal government security engagements.
- Experience supporting the national efforts engaged in the continuity of government and continuity of operations planning.