

convergence technologies. However, the companies that can bring this expertise to the table are still in the minority. The low competency of some security integrators and their inability to service the IP-based technology they sell may be the most common complaint we hear.

The decision maker's exposure to IT-based technologies.

The insights many decision makers have into security technologies are limited to presentations from vendors. However, this is changing as more districts and institutions move toward these technologies.

Cost of purchasing and installing the equipment.

Certainly the cost of IP-based devices continues to fall, and the quality of the devices continues to improve. Nowhere is this more apparent than with IP video cameras. Image quality, device management, GUI functionality and friendliness, and other enhancements have made IP video very useable. However, IP cameras still represent less than half of cameras installed.

IT infrastructure and bandwidth concerns.

Sometimes the most obvious questions are not addressed until financial and operational commitments have been made. The quality of network infrastructure is one of the major factors that will determine your satisfaction with IP-based security technologies. Before you consider using the institution or district's LAN/WAN for security data, answer the following four questions.

- Is the network reliable? Short periods of downtime for organizations that rely on their network for e-mail, Internet access, and non-mission-critical applications are not usually problematic. However, security management and monitoring are mission-critical functions. Disruption of alarm monitoring or CCTV could result in significant security breaches. Consider:
 - How are OS patches, software updates, and security updates managed? Do they require system downtime?
 - Are there single points of failure in the network architecture?
 - Where are redundant communication strategies required?
- Is the network survivable?
 - What happens if a fiber optic cable is destroyed by a backhoe or a switch is destroyed due to a power surge?
 - Is the network self-healing?
 - Are network problems immediately and automatically communicated to technical support through SMS messaging?
- Is the network sustainable?
 - Are all critical network components on UPS with generator backup?
 - What are you going to do when the generator runs out of fuel?
 - Are critical security devices on emergency power?
 - Have generators been tested under load?
- Is the network configured for both logical and physical security?
 - Are data closets secured or are they shared with housekeeping or storage rooms?
 - Are OS, switch firmware, and application security patches current?
 - Are intrusion attempts, both physical and logical, monitored and addressed?

IP security technologies that were "bleeding edge" just a few months ago have moved into the "leading edge" category, but there are still many challenges to be faced in the implementation of these technologies.

How to Make Your Convergence Experience Powerful

The school administrators and security professionals I spoke with related a wide range of experiences as their organizations moved toward converged security technology platforms. Several institutions reported conflict between IT security and physical security staff. Others described evolving relationships based on common organizational goals. In other instances, particularly in those organizations without an in-house security professional, IT staff is taking a leadership roll in identifying technology opportunities and strategies and funding the infrastructure needed to integrate these.

Based on the experiences we have observed, here are the top things your organization can do to more effectively implement convergent security technologies.

- Base your security technology plan on a thorough assessment. Be sure to involve key stakeholders, as appropriate, throughout the assessment process.
- Articulate why each device is being installed and what you expect to accomplish with it.
- Develop a security technology master plan that includes the establishment of operational and technological priorities to guide you in future purchases.
- Focus on functionality, not jargon. Be careful of phrases like "capable of," and "can be." They often imply that additional hardware, software, or options are needed. You have the responsibility to understand what you are buying and to ensure the technology meets your needs.
- Specify in writing how you expect the system to work. For example, if you want five seconds of pre-alarm video to be displayed on the access control system client workstation when an alarm is reported, the specifications document should clearly state this.
- Establish a partnership between the security program and IT professionals now. Do not wait until a project is in the planning stages or a significant incident has occurred to begin the process. This relationship will be critical in the future.

- Think standards. Unlike most traditional security systems, IT technology is standards based. Infrastructure architecture design, cabling, programming, and network switch configuration have to be done by professionals. If you expect to use your organization's WAN/LAN for (security) data transmission, you need to comply with these standards through the design and installation process.
- Technology integration can increase the overall effectiveness of your security systems. Plan for this from the beginning and ensure that your technology purchase and installation decisions support your plan.
- Work collaboratively with the Facilities, IT, and Purchasing departments to ensure all security technology purchases fit into your security technology master plan.
- Clearly outline your expectations to your security integrator, and hold them accountable for performance, installation, and service.
- Ensure your LAN/WAN is sustainable, survivable, reliable, and logically and physically secure.
- Address issues such as OS, security, application patches, and downtime procedures when you design the infrastructure.
- Develop policies and procedures related to data access and public records before you are challenged. This should include an appropriate records retention schedule. In many instances, these policies will need to be approved by the school board or board of trustees. These policies should be in place before the system goes live.

The convergence of traditional security technologies with IP-based technologies will provide phenomenal opportunities and challenges to school systems, private schools, colleges and universities. Missteps can be costly but are often avoidable. When organizations work toward common, well-defined goals and ensure that security, IT, facilities and construction professionals work together and embrace these goals, the likelihood of success is greatly improved.

However, if after the first meeting between your security integrator, the security administrator, and your IT department, you are convinced that one is from Venus and the other is from Mars, call a time out. It is vital to the success of the project that all these individuals speak a common language, understand the design and installation standards, have a common set of goals, and respect each other's operational and organizational needs and responsibilities. Following the steps outlined above, working with a competent security integrator, and focusing on the security/IT partnership are the best ways to make every project successful.

Elliot A. Boxerbaum, CPP, CSC is president of Security Risk Management Consultants Inc. (SRMC) and has been consulting since 1989. His career includes campus and public law enforcement and senior management positions in both private and public security organizations. He has authored numerous articles and is a frequent speaker at national seminars on security assessment, planning, and technology design. Mr. Boxerbaum is a member of IACLEA, serves on the ASIS International Healthcare Security Council and Physical Security Guidelines Development Committee, and is vice president of the International Association of Professional Security Consultants. He can be reached by at ElliotB@S-RMC.com or 614-224-3100. For more information about SRMC, visit www.S-RMC.com.

Printable version may be for personal use only. Content may not be duplicated, re-used or otherwise replicated without expressed, written consent from SecurityInfoWatch.com and/or the original author/source.

Visit SecurityInfoWatch.com - The Complete Information Resource for the Security Industry.
