Selecting Security Technology Providers

National Clearinghouse for Educational Facilities

Tod Schneider
2009

This is a companion to the NCEF publications School Security Technologies *and* Mass Notification for Higher Education*.*

Overview

The world of security technology holds great promise, but it is fraught with opportunities for expensive missteps and misapplications. The quality of the security technology consultants and system integrators you use will have a direct bearing on how well your school masters this complex subject.[1]

Security technology consultants help determine your security technology needs. *Systems integrators* design and install the appropriate hardware and software to meet those needs.[2] There is often overlap between consultants and integrators; most consultants were at some point integrators and installers themselves. The distinction is that a consultant acts as a neutral third party, serving as your advocate and protecting your interests as you wade into the security technology maze. Select a consultant first; the consultant will help you find the right systems integrator.

Selecting a Security Technology Consultant

Security technology consultants should be independent, with readily verifiable references and projects in your area that are currently operational and similar to the one you have in mind. Obtain recommendations from facilities and information technology (IT) staff at schools and other institutions nearby, as well as from manufacturers, integrators, and installers of security technology products. *Ask for full disclosure if the recommended consultants have commercial ties to these entities*. References are critical and should be based entirely on performance. Select the consultant whose experience and personal qualities best fit your requirements.

The consultant will have two primary tasks:

- Assess your school's security technology needs, working closely with security, facilities, and IT staff. Use Appendix A, *Identifying Desired System Attributes*, and Appendix B, *Identifying Desired System Components,* to aid the assessment process.

- Help select and supervise a systems integrator.[3]

Selecting a Systems Integrator

Your security technology consultant will have a good working knowledge of the systems integrators in the area. The schools and institutions you contacted earlier should have additional recommendations. For large or complex installations, only a handful of integrators may be qualified for the job.

You will be entering into a long-term "marriage" with the systems integrator you choose, so it pays to conduct a rigorous selection process.

1. Pre-qualify candidates. Prospective firms should provide the following information:

- Company documentation, including how long it's been in business, its core competencies, key personnel certifications, and clientele.

[1] Read the **Look before You Leap** section on page 1 of *School Security Technologies*.

[2] Integrators use installers to put system hardware and software components in place. Installers may specialize in one component, such as cameras, while the integrator keeps an eye on the big picture, ensuring all components are compatible and interlinked. Installers may be independent subcontractors, but preferably they are employees of the integrator, making it much easier to pin down who has responsibility for maintenance, repairs, or adjustments down the road.

[3] If you already have a systems integrator and are happy with its performance, you may not need a consultant. But if regulations require you to seek bids for new services, you may need to bring in an outside consultant to avoid the conflict of interest inherent in having the integrator write and bid on its own proposal.

■ At least five customer references for similar systems in the area, preferably with five years or more of service to each.
■ Assurance from each reference that their systems work as promised, and that follow-up maintenance and repairs have been satisfactory.

2. Conduct site visits. Arrange a site visit for each firm. Provide site maps, building layouts, and schedules for everything that must be accommodated, such as doors, electronics, and hardware. Discuss your security objectives, problems, and concerns, as well as potential solutions being considered.

3.Clarify your needs and expectations. Following the site visits, clarify your needs and expectations and state them succinctly in a written request for proposals (RFP). *The clearer the RFP, the better the proposals will be.* Lowest cost should not be the stated concern — it's the system performance that counts. A cheaper system will be worthless if it fails to provide the performance you need for the security you seek. The value of long-term system reliability far exceeds any short term cost savings. In fact, an unusually low bid can indicate that the proposal is unrealistic or the applicant doesn't fully understand the your needs. (See the *Affordability* section in Appendix A, below.)

4. Invite proposals. Issue the RFP, requiring each firm to submit a detailed security technology proposal, including spec sheets, product descriptions, installed costs, and annual operating and updating costs.

4. Demonstrate each proposal. For each proposal that looks promising, ask for a demo. This could involve demonstrating a similar system nearby or bringing in equipment to your school to test, using the same software and hardware cited in the proposal.

Demonstrations should be attended by school facility, safety, maintenance, and IT staff. The demos should go beyond watching the integrator use the equipment, allowing staff a hands-on opportunity to try it themselves. If, for instance, the initial test involves sending a broadcast message to students, try adding other groups — such as school personnel and local emergency responders — to determine the system's flexibility and scalability.

It's important that you find the system easy to use. Under pressure during a crisis, your ability to handle complex operations will be seriously limited.

5. Rate the proposals. Establish a rating system for comparing proposals.[4] For example, a 100-point system might be:

■ *15 points*. The skill, experience, and record of the firm in the performance of similar types of security systems.
■ *40 points.* The quality of system design and performance (for example, recorded video resolution, system configuration, technical features of system equipment) along with the level of the firm's understanding of the extent and scope of the work to be performed.
■ *25 points.* The proposed system's price and installation rates.
■ *15 points.* The firm's financial stability and ability to provide ongoing warranty and service support after the installation.
■ *5 points.* Any other factors considered relevant.

Designate two or three staff members to sit with the school's security technology consultant and evaluate the proposals, assigning scores to each proposal and awarding the work to the highest-scoring firm.

Additional Information

See the NCEF publications *School Security Technologies* and *Mass Notification for Higher Education*.

Publication Notes

First published in April 2009.

[4] Schools are usually permitted to use such a rating system in lieu of "low bid" for selecting security system vendors. This provides decision-making control over the selection process, whereas a reliance on low bid takes authority out of the school's hands, forcing it to accept any system that marginally meets minimum specifications.

Appendix A
Identifying Desired System Attributes

Essential characteristics of a new security technology system should include the following:

Convergence. Although technological solutions can be installed as free-standing devices, in most institutional settings it makes sense not only to build an integrated system, but to build it from the ground up on the same platform. This is the most cost-efficient approach, and it helps avoid the technological glitches found with incompatible software or hardware. An integrator chooses components specifically to ensure they are compatible. The end result should minimize the amount of training, maintenance, data base management and software support necessary. Typical components of an integrated system include access control, surveillance cameras, and intrusion detection systems (IDS), all tied together for maximum effectiveness. They could be linked to data bases, visitor badge and proximity card creation, intercoms, and biometric devices. It's not enough to state in an RFP that components must be compatible — your security technology consultant must verify that they are. If an integrator suggests a system that comes with an "SDK" (software development kit), that means you have to write your own software; this is both time-consuming and expensive, commonly running $10,000 or a great deal more.

Ease of use. The system should work seamlessly with your existing intranet and should be easy to use, particularly under high stress circumstances. The displays that appear on computer screens (GUI's, pronounced "gooeys", or graphic user interfaces) should be simple to use by authorized users with minimal training. Large user manuals are a red flag — workers should find it easy to fulfill their roles when a crisis occurs without having to dig through a manual. The process for maintaining and updating data bases of student or staff contact information should be addressed. For example, students should be able to update their own information on-line without difficulty. Contact information changes so frequently that keeping it up to date should be a high priority, or even the best system will fall short. In a worst case scenario, live help should be available by phone 24/7.

Accessibility. Multiple workstations should be able to tap into the system simultaneously from various locations. In many cases, Internet access should be used to allow authorized users to send messages or view images from anywhere in the world.

Flexibility and Scalability. The system should be able to grow as hardware and software evolves. It should be able to add new hardware, such as more card readers and cameras, and it should be able to send messages to newly created communication devices in the future. It should also have some redundancy and backup power, in case of technical glitches or power failures. (Have a plan B for a worst case scenario, such as when cell towers fail due to extreme weather or vandalism.)

Capacity. Various factors affect how large a volume of information can be sent out at once, or within a reasonable period of time. For example, the local cell tower, area infrastructure, and service provider capacities can be limiters. Phone lines are commonly jammed during a crisis. You may have to establish formal working relationships with service providers to arrange priority delivery of emergency messages on a mass scale.

Sustainability. An integrated system is a long term investment., so it is essential that upkeep be considered. There should be a maintenance agreement (MA) with the integrator in most cases. A "pay as you go" approach is usually more affordable, although a comprehensive agreement is also an option. Provisions for a software support agreement (SSA) are also essential. Without an SSA, when software glitches occur the whole system can fail.

Diversity. A good system should be able to quickly deliver messages in any relevant languages, orally and visually.

Fringe benefits. Recent improvements in many emergency notification systems (ENS) allows them to be used for notifying parents about absences, surveying families for feedback, or fulfilling other non-emergency functions.

Affordability. Don't confuse up-front costs with long-term affordability. System quality is far more important than system cost , so resist the temptation to go with a low bid. There have been a remarkably high number of project disasters that were blindly driven by low bids. The companies involved were generally in over their heads, couldn't deliver what they promised, and frequently ended up going out of business before completing the job. Schools ultimately had to re-bid, spending far more than they would have if they'd chosen a more realistic bid in the first place. Pin down details, such as whether you're paying for unlimited service or are charged a hefty fee every time you send a message.

Appendix B
Identifying Desired System Components

Here are just some examples of possible technological solutions you might identify for your campus. See the NCEF publications *School Security Technologies* and *Mass Notification for Higher Education* for more information.

Emergency notification throughout the campus, via:
- Siren
- Loudspeakers or intercoms
- Electronic message displays

Emergency notification to selected individuals and groups, via:
- Cell phones
- Email
- Text messaging

Cameras with specified capabilities, such as:

- Capturing license plates or faces under specified conditions at specified locations
- Storage capability for a minimum of ten days
- IP (Internet protocol)-based, with PoE (power-over-Ethernet), or wireless mesh systems
- Intelligent-video capabilities, such as triggering alarms when restricted areas are entered

Surveillance over hidden areas, such as:

- The rear of the library
- Inside parking garages
- In an alley next to the dorms

Surveillance over other areas of concern, such as:

- Locations where problem behaviors have occurred in the past
- Access points to research labs
- The visitors' parking lot
- Pedestrian passageways used late at night
- Areas where cash is handled, including the registrar's office and ATM machines

Emergency alarm options, such as:

- Panic button alarms in the dorms or along isolated walkways
- Portable alarms for students who request them
- Fire, chemical and biological alarms

Intrusion Detection Systems (IDS), such as:

- Alarms that can send messages regarding intruders
- Virtual fences, that detect intruders
- Alarms triggered by door, gate or windows being opened
- Alarms reasonably armed or disarmed by all appropriate staff at all hours

Access Control systems, such as:

- Proximity card door controls that record identities of door users
- Anti-piggyback revolving doors that prevent unwarranted entry.
- Biometric readers