Living
On Campus:
2007 College Housing Report

2007 Education Design Showcase Awards

Restroom and Locker Room Furnishings

Window Shading Systems

Safe Campus Checklist

By and large, schools and colleges are safe places. But in the wake of the recent tragedy at Virginia Tech and the eight-year anniversary of Columbine, educational institutions are searching for new, more effective ways to protect their students. While tragedy often brings out the best in people, it also brings out the worst. New security companies and consultants are popping up everywhere — many with no experience or real expertise. To help schools and colleges just beginning to discover the world of security technologies make informed decisions, College Planning & Management and School Planning & Management have partnered with experts in the field to develop a checklist outlining the points to consider when purchasing security services and equipment.

Company Background

- ❏ Check pedigrees. Make sure the provider is legitimate, experienced, and qualified.
- ❏ Whether you are looking for a service or a manufacturer, make sure they have been in business for at least five years, operating under the same name and management team.
- ❏ Meet with a senior manager of the company and, when practical, visit their facility. Make sure it is obvious they are not just a shell operation.
- ❏ Ask for a list of references that are related to your application, and check them. Make sure the references are legitimate, not just another retained consultant or "family friend."
- ❏ Assemble customer contact information, and arrange client visits if possible. When visiting a customer, talk to security management personnel, system operators, and system administrators. Find out if they're satisfied with the systems integrator. Determine the level and responsiveness of customer support and the quality of maintenance. In other words, get as much relevant third-party input as you can.
- ❏ Do your due diligence. Check for outside information on the company and its services or products in the media or through Google, blogs, etc. to verify credibility. Read testimonials or quotes from other customers.

- ❏ Ask if manufacturers and their distributors act as a team for end-user support. If the provider is local, do they have regional or national credibility and support?
- ❏ Don't be afraid to ask for a financial history to assess for yourself if the company is economically sound.

Education Experience

- ❏ How many years has this company been in the education market? Ask how many installations they have in educational institutions and ask for references from these institutions.
- ❏ Look for a provider who has knowledge of how their equipment is best used in educational environments. It is important that the provider understands not only his own equipment but also the specific application to schools and colleges.
- ❏ Look for companies that are invested in education and have training and knowledge that is specific to the issues encountered on a campus (e.g. alcohol abuse, young adult behavior, Family Educational Rights and Privacy Act [FERPA], Jeanne Cleary Act).
- ❏ When it comes to access control, look for providers who understand the different needs of day-to-day screening versus total screening at special events such as athletic contests.

Qualified Personnel

- ❏ Determine the exact skills and background of the team that will be assigned to your account — executives, site managers, and staff — and the company's commitment to ensuring customer satisfaction and quality.
- ❏ Look for active oversight and an ongoing relationship with great contract manager-contractor relations as part of your agreement.
- ❏ Ask what system platforms the integrator installs and services and how many trained technical staff there are in the organization. Find out if the integrator has employees who are Microsoft-certified software specialists, CISCO-certified networking specialists, and Certified Protection Professionals (CPPs). Ask

how many other clients have a system similar to the one that will be installed at your site. The answers to these questions will help you determine the integrator's strength and ability to support you.

- ❏ Ask the integrator for training records, such as product training certificates, and inquire if the integrator provides recurring training for its personnel. Don't limit yourself to meeting with just sales personnel. You should also interview management representatives and technicians as part of the proposal process. Probe your candidates for anything else you can think of that will help with your choice of a systems integrator. If your organization has other sites that may be looking to install or upgrade a security system, check out whether the systems integrator has offices around the country with security system installation and maintenance capabilities. The bottom line is this: You are the customer, so be demanding. In the final analysis, a quality integrator is one who will meet or exceed your expectations.

Contract Service Providers

- ❏ It's vital that any security company engaged for campus security programs be committed to enhancing their technical skills and industry/segment knowledge through comprehensive training programs that are tied to employment goals (promotions, raises, etc.). The most important resources of any security services company are the people, and it is vital that they are continually engaged, comprehensively trained, and provided with incentives to achieve and excel.
- ❏ For contract security specifically, it is vital that the contract security firm have the ability to appropriately vet the assigned resources through background checks (employment and criminal records) and drug tests.
- ❏ Clients can ensure that disruptive staff turnover is minimized if their contract security firm is committed to having a comprehensive recruiting, training, compensation, and management program.

Certifications and Warranties

- Check the product warranty. Many products carry a lifetime warranty. Also, check the warranty on the installation of important safety products.
- Find out if the manufacturer stands behind their warranty. What is the length and content of the warranty for each project?
- Only buy equipment that is certified or meets the specifications of national or international governmental agencies.
- Look for companies that use nationally recognized standards in their technology and/or delivery of professional services (e.g. SAFETY Act Certification through the U.S. Department of Homeland Security, ISO-certified companies).
- Check flammability ratings and review independent approvals (UL, etc.).
- For a manufacturer, get their in-warranty failure data on the products you are considering and make sure it is best-in-class for that product category.
- Find out who to call if you need onsite visits, training, and warranty replacement, and how to get service after the sale if there is a problem.

Questions About Product

- When it comes to security, remember that there is no one-size-fits-all solution. To implement the due-diligence process, you need a plan that includes a description of the issues to be solved, a list of those who have a vested interest in system implementation, and an overview of who will be responsible for the system. The plan should include a scope of work and system specification.
- All too often specification writers and decision makers find it easier to look at features that do not enhance performance and sometimes are used outright to mask deficiencies in a device. Make product decisions based on performance, not features.
- Always ask: have the company's products/services been used in actual incidents, not just drills or pilot deployments?
- How well do products perform in terms of reliability? Are they designed and constructed to withstand constant usage, abuse and vandalism? How robust are the products (e.g. strength of bolts and latches)? What

type of product testing has been conducted?
- How vulnerable is the system to inclement weather conditions? What is the operational temperature range (will it handle your high or low temperatures)? Does it have UV stabilization against sun deterioration (will products fade in the sun)?
- Would the system still work during a power failure? How easy or difficult would it be to cut wires or disable a system? Does the system offer redundancy? Are the systems self-healing and self-configuring?
- Does your notification system support on-demand audio/video messaging (pre-recorded announcements) and live broadcast (real-time instructions)? Can it deliver the message to any location (e.g. television, PC, wireless device, cell phone)?
- How easy is the system to install, manage, and maintain? Is the system scalable — allowing for growth and the integration of new technologies? Can it tie into the existing IP network to ensure maximum reach and flexibility?
- Following an emergency, campus security personnel need to rapidly understand what happened and why, and collaborate with law enforcement agencies to share this intelligence. Can your system quickly contact decision makers and get them up to speed so next steps and action items can be executed as quickly as possible? Does it have audit capabilities? Is it possible to give law enforcement officials complete access to information from the school security system? Can the system be tied into the local 9-1-1 call center?
- Are you currently monitoring one or more locations at your university? Are you using card-based access for campus facilities? What student information system is in place, and how are housing assignments managed? These may seem like far-lying systems, but each can create a powerful integration with other security systems. Take into account the technology that is currently in place on your campus, and look for a provider that can integrate with these other systems to provide comprehensive connectivity.

Questions About Ownership

- Which department will be managing your security system? What is the makeup of

its employees, and what is their current workload? What is their level of experience with technology similar to what you will be implementing? Will IT be involved at all? You must consider the end-user throughout the purchasing process. You may find a system that does everything you are looking for, but without the proper personnel in place to keep it running smoothly, it won't matter. Take another look at customer references with demographics similar to your own. Are the system operators in highly technical roles? How much time is spent configuring the system vs. monitoring it? The makeup of your department will affect how well each type of technology is utilized.

Total Cost of Ownership

- Some companies will come in with low upfront costs and then have very expensive ongoing proprietary card or consumable costs. Or they may give away the software or offer it very inexpensively in order to tie you to their more expensive proprietary hardware. How well does the solution integrate with your existing technology? Is it just another application on an administrator's workstation, or does it require a separate and completely dedicated workstation? Is the system easy to expand over time, or will you need to buy everything now even if you will not use it for two or three years? These are questions you must ask in order to discover the true cost of the system.