Understanding and influencing the design process for health facilities
Jay King, CPP, PSP

Safety and security directors’ perspectives and advocacy are essential throughout the design and construction processes, the author contends, stressing that they can have the greatest influence on a project before the design team is even selected. In the article he describes the five ways that the process can be influenced before it starts, avoiding the possible spending of decades, and hundreds of thousands of dollars, trying to overcome insufficient attention having been paid to security program requirements during the facility design process.

(Facing page)

FIVE WAYS TO INFLUENCE THE SECURITY DESIGN PROCESS BEFORE IT BEGINS

“So, where do you want your cameras?” This was a question posed to a hospital safety and security director during the schematic design phase of a large healthcare facility construction project. It is significant that the designer asked the security director, but at that stage of the design, whatever response the director provided would have been less impactful if he had been included much earlier in the design process. A healthcare facility’s security department may spend decades, and hundreds of thousands of dollars trying to overcome insufficient attention having been paid to security program requirements during the facility design process.

An image of a person pouring over CAD drawings and specifi-
cation documents may come to mind when one thinks of what is involved in a design review. However, if a security director enters the design process after the design begins; whether the drawings are at 30, 60 or 90% of completion, any changes or improvements the director suggests may be costly and may come at the expense of other facility requirements or building systems. Further, some security concepts like Crime Prevention Through Environmental Design (CPTED), or increased building standoff to mitigate against vehicle threats, each involves the physical orientation of entire facilities within project site boundaries. When building drawings are being drafted, it is too late to significantly influence these important site security considerations.

The safety and security director is the facility's resident security advisor; the director will use the security systems being designed to protect the people for whom the facility is being built. A safety and security director's perspective and advocacy are essential throughout the design and construction processes; however, safety and security directors can have the greatest influence on a project before the design team is even selected.

There are five ways that the process can be influenced before it starts:

1. Design Guidelines or Standards
2. Assessment and Physical Security Master Planning
3. Exercise and Incident Reporting
4. Architect and Engineer Selection (RFQ)
5. Programming Phase

**USING OR DEVELOPING DESIGN GUIDELINES OR STANDARDS**

Design guidelines or standards enable facility managers and security directors to conceive of an ideal facility before the project planning, procurement, or design processes begin. Design guidelines allow organizations to depict and describe the preferred facility design based on operational requirements. General safety and security risk-based design requirements, equipment, and materials for the site, as well as facility and room types are usually included in design guidelines. An organization may include example floor layouts; even entry
door elevation diagrams, allowing facility stakeholders and prospective designers to envision the facility well before a project is initiated.

Unlike many other industries, the healthcare field does not want for design guidelines. The American Institute of Architects’ Academy of Architecture for Health and the Facility Guidelines Institute have published thorough design guidelines for different types of healthcare facilities; these resources include important basic security requirements for these facilities. IAHSS has also made a meaningful contribution with its *Security Design Guidelines for Healthcare Facilities* publication.

The challenge for security directors (in the healthcare industry, at least), is not to re-create original designs guidelines, but rather to understand the existing guidelines, and interpret them for their own organizations’ unique operational and security program requirements.

This is important for two reasons:

1. When a new facility or upgrade project is planned, procurement teams will use these guidelines to develop design requirements to include in Request for Qualifications (RFQs) or other procurement documents. They may also base rough design and construction project budget estimates on these requirements. If healthcare facility security design requirements are not adequately addressed in an organization’s design guidelines, it will be a more of a challenge to cram them in after a designer is selected, and the project has begun.

2. When a security director answers the question, “where do you want your cameras?” with his own opinion, it is only as impactful his own experience and credibility. When that opinion is bolstered by citing the respective paragraph of the industry or organization design guidelines, his opinion is much harder to second guess, and he contends with designer in language that the designer appreciates. A security director can add real value to his organization’s project team by ensuring that the security-related goals of the industry or organization design guidelines are acknowledged and implemented in design process.
ASSESSMENT AND PHYSICAL SECURITY MASTER PLANNING

A separate process which can inform design requirements is the risk assessments that security directors already undertake. A final result of most risk assessments is the mitigation recommendations. A report of some type will include recommendations for improvements in planning, staffing, training, equipment, and also design. There will be risks which can be addressed with improved access control, alarms, video surveillance and communication equipment (duress or public address). Risk assessment reports should not be allowed to accumulate over years without their physical security design and system improvement recommendations being expressed in actual facility design.

If you are looking for a new risk assessment methodology, wait 60 days. Someone will invent one. IAHSS previously offered its own Risk Assessment Toolkit, and the American Society for Health Care Engineering of the American Hospital Association offers similar tools. Whatever methodology is selected, it should be transparent and recognized by the organization’s industry. Preferably, the methodology should be non-proprietary; and its results or final report should never require the aid of consultant to interpret.

The Risk Assessment Team. The composition of the risk assessment team is just as important as the right methodology. Too often the task of completing risk assessment is confined to the security department, and the audience for the final report and recommendations is not much broader. The engagement of other departments for risk assessment teams if often superficial at best.

Involving many other departments in a risk assessment (including a representative from the department that will authorize or fund the risk assessment mitigation recommendations) is an important step in creating a consensus report product; and the process itself can build awareness and intra-organizational buy-in for security program goals.

An important bridging document between design guidelines and risk assessment reports is a physical security master plan. A risk assessment report may yield
a laundry list of mitigation recommendations that are too costly to implement in a single budget year; design improvement recommendations can often require the greatest investment. A master plan will distribute design and other recommendations over multiple years, focusing on the most critical risks first. The master plan will pair recommendations with actional implementation steps and will align security program design objectives with industry design guidelines, in parallel with organizational funding cycles. Thorough plans for incremental improvement are usually more persuasive to senior executives that the “tyranny of the urgent”.

This risk assessment and master planning effort will serve the security director in the design process for two reasons:

1) Many of the same department leaders who are members of a risk assessment team are very likely to be part of project teams which oversee design requirements for new or expanded facilities. The security department will compete with other departments for priority and resources when a design project is planned.

It will be harder for team members department’s representatives to dismiss the risk issues which are driving physical security design requirements when some of the same team members’ names appear on the cover of the risk assessment report.

An inclusive risk assessment process can create consensus for security design improvements before the project is initiated.

2) Another important outcome of a risk assessment is the inevitable creation of “foreseeability”. Whether an incident is foreseeable includes the legal requirement that the “consequences of a party’s action or inaction could reasonably result in the injury…the resultant injury was reasonably predictable by a person of ordinary intelligence and circumspection.” All healthcare facilities have risks, and the risk assessment process will document many of them. Such documentation may be discoverable in related future legal proceedings.

It is difficult to argue that an incident was not foreseeable when a risk assessment document prepared by an inter-departmental team may suggest otherwise. From this perspective, actually
implementing physical security design recommendations within a reasonable period of time may not only improve the safety of people using a facility, but it may also have bearing on an organization’s long-term liability.

EXERCISE AND INCIDENT REPORTING

A mature healthcare facility safety and security department will have a well-developed exercise program that tests the capability of the department; and even the most recently established department will have implemented some form of incident reporting system. Regrettably, exercise after action reports, or incident reports are not often mined for data to justify design requirements, or to improve design guidelines.

After action comments like “Team A could not communicate with dispatch via radio…”, or “Post B did have line of sight to the intrusion site…” both suggest issues that can be mitigated through improved design. In the first case, an additional radio repeater, and perhaps a tower or pole, is required at another location on the property. In the latter case, improved landscape design may solve the issue. Exercise scenarios can also be crafted as a “proof of concept” for recommended surveillance or communications technology improvements.

Improving incident reporting can also enable design enhancements. A security officer’s report will record UCR crime information, but seldom are environmental clues included. An auto burglary in a distant part of the healthcare facility’s parking area is not a critical incident, but details about the lighting, vegetation, and sight lines of the area surrounding the vehicle will suggest opportunities for design improvements which can deter future burglaries.

Design guidelines and assessments are important, but the outcome of exercises conducted by actually facility staff, on the facility site; or recent local crime trends or crime scene environmental information can be especially compelling in justifying design requirements.

ARCHITECT AND ENGINEER SELECTION (RFQ/RFP)

The selected architect and engi-
neer team will implement the security director’s design requirements, so it is critical that the security director be involved in the procurement process that selects this team. A Request for Qualification or Request for Proposal (RFP) will include a performance work statement (PWS) or a scope of work (SOW) which described the work to be completed. The RFP will also include an evaluation section which explains to prospective bidders how their proposals will be evaluated by the selection team. The evaluation section is usually a matrix format, with a scoring system for ranking the content of proposal submissions.

The security director should insist on writing or closely reviewing the security-related portion of the RFP’s PWS; security design guidelines should be cited or referenced wherever appropriate. Just as important as shaping the PWS is carving out a place in the proposal review matrix for ranking the security design qualifications of prospective bidders. Bidders will infer from this matrix what the healthcare organization considers most important in the project.

If points are available to award for security design qualifications and past practice, procurement teams are likely to include the security director in selection committee’s proposal review process.

A security director’s obvious involvement in crafting the RFQ or RFP will inform A/E firms making bid/no bid decisions; they will be forced to appreciate that the organization is serious about security. If an A/E firm lacks the security design qualifications they may elect to not bid, or they may add a sub-consultant who can help them close this capabilities gap. In either case, the selection committee will receive proposals that address or even emphasize firms’ security design qualifications, and whether they have past practice demonstrating their ability to do the work. Ideally, the selection committee receives proposals from firms that are all serious about security so that the security program benefits no matter which firm is selected.

Beyond just helping select the most qualified firm, the security director also has a role to play in effecting the operational security (OPSEC) of the procurement process. Because procurement
documents and concept drawings may reveal security gaps or vulnerabilities, many organizations separate the security design requirements portion of the RFP from the other RFP sections. Security design requirements are provided to bidders only after signing a non-disclosure agreement (NDA) and describing their firm’s handling procedures for sensitive security information. This extra step does not guarantee information security, but it minimizes the likelihood that security vulnerabilities are exposed via publicly accessible procurement websites.

The security director’s management of the NDAs and procurement OPSEC is also another way to remain involved in the procurement process, and to be kept abreast of interested firms which submit proposals.

PROGRAMMING PHASE

After the selection committee chooses the best qualified firm, the design programming phase will precede the schematic design phase.

Design programming typically involves a series of focus group-type meetings led by the A/E team. The goal of these meetings is to compile a list of owner requirements for the design project from a guided discussion with the organization’s key stakeholders.

For security directors, information about specific device numbers, equipment placement and technology manufacturers are welcome, but not essential during design programming. Instead, a security director should clearly define what he/she wants systems and device types to achieve, and in what areas of the facility he/she wants them to achieve these ends. Risk assessment and incident reports will document why he/she wants to achieve these outcomes.

In only one significant way are design programming meetings like any of the other hundreds of meetings that stakeholders will endure in their careers: the outcome of the meeting will tend to favor the most prepared attendee. Programming meetings will help define the design of the site and facility that the organization will inhabit and be responsible for maintaining for the next several decades (or more), they should not be treated like just any other meeting.
Fortunately, the security director who has: (1) helped develop security design guidelines, (2) led interdepartmental risk assessment and master planning teams, (3) reviewed exercise and incident reports for design requirements, and (4) been thoroughly involved in the selection process for the current A/E firm, will be well prepared to define design requirements which benefit security program goals, and to support them with objective justifications when there is competition for project resources.

CONCLUSION

After design programming, the schematic design phase commences. At this point, the security director’s interaction with the A/E firm is more circumscribed. He/she should remain involved at each design phase review, but design change recommendations are submitted for approval via a project manager or owner representative. The challenge and cost of effecting design changes increases as the design process progresses.

If a security director has engineered the above five steps within his/her organization, he/she enjoys the advantage of having an A/E firm that excels at security design being assigned to implement well-defined security design guidelines, which specifically addresses risk issues that the facility’s healthcare professionals may face. The question “where do you want your cameras?” (and access control, alarms, duress devices, etc.) is answered before it is asked.

Sources: