



How to Get the Most Out of Your Security Design Process

The security systems you have had in place for the last decade may have provided excellent value for years, but will not necessarily meet your current and future security and safety needs. How do you update platforms to provide additional reliability and help reduce operating costs and save time? This paper will discuss how to get the most out of your security design process.

Three Common Approaches to Security Design and Implementation

There are many options available to accomplish the task of security design and implementation. Generally, the choices can be summarized in three primary methods:

// Option 1: Do it Yourself

// Option 2: Hire a Consultant

// Option 3: Partner with a Security Integrator

// Option 1: Do it Yourself

If your company has the expertise to choose this option, including design and system specifications, you can issue an RFP. Either use a performance based specification that describes what the system must be able to do, or issue a product based specification listing specific products to be used.

Pros-

1. By doing the design work on your own, you get the least expensive option - with the cost of the design minimized. The total cost of the design includes the "opportunity cost" of the in-house security department dedicating time and resources to the system design vs. other job tasks. Some of the components of the design effort can be leveraged with "normal" security functions, including a site survey and risk assessment.
2. The design task can be fit to any allotted time available in the security project schedule via internal prioritization.
 - Scenario A: A warehouse experiences a break-in in an area where no existing video surveillance coverage exists; the CEO ordered a system to be placed within two weeks.
 - Scenario B: A warehouse has never experienced a break-in, and although a video surveillance system has been in place, budgets are tight and this quarter the surveillance will lapse.
3. You have total control of the design element. You can get exactly what you want, provided you know what to ask for in a clear and precise manner. This approach is not for the beginner.

Cons-

1. You are "on your own" and must rely solely on your knowledge and experience or that of your company's resources. There is no way to vet design elements, so you and your company assume all of the risk for design flaws, product choice and interoperability of subsystems.
2. The design phase can be delayed if "normal duties" continually interfere with design tasks, in part because it is not the core component of the security department's daily responsibilities.
3. When you assume the consultant role and multiple vendors are involved with the project, you are responsible to ensure that all of the equipment, subsystems and integration of scope of work (SOW) will provide a complete system. Ensuring that the SOWs for all vendors are equal to a complete and functioning system becomes your responsibility. You then take on the role of project manager, as well as consultant.

Following is an example where a wrong approach was detrimental to the project. The project manager for XYZ Company made the decision to split up a security project into three logical components that were awarded to three different vendors: One vendor for head end programming, a second vendor for field equipment installation and connection, and a third vendor for system infrastructure (AC power, wiring and conduit). At the end of the project when all three vendors completed their respective SOWs,

an issue arose in which the system did not have the ability to read XYZ Company's cards. XYZ Company had overlooked a critical portion of the project - none of the contracted vendors was responsible for ensuring that the system had the ability to read a card and provide access. The project manager did not recognize the gap as the work scope of the project was designed, and the result was finger pointing. The project manager did not fully understand the tasks required to ensure that the system would be capable of allowing access to authorized cardholders.

// Option 2: Hire a Consultant

A security consultant will provide you with consulting services, system design, and assistance in evaluating bids. You can do this if you do not have an internal resource with deep subject matter expertise and need guidance, but it will cost you to utilize this expertise.

A consultant can reduce risk and can add an objective view in selecting a platform that best meets the customer's needs. However, be aware that they can only recommend products they are familiar with. Consider that a fair portion of budget spent on consulting fees could be allocated to security products and services.

Contracting with a consultant is highly recommended for projects that will involve multiple trades, including construction projects with a complete building retrofit. It is also beneficial when you are required to manage a mass of details that are not security system related but impact the security system design and deployment, such as the implementation of electrical, security, IT, telephones, etc.

Utilization of an industry standard approach is another benefit of using a security consultant. Specification sections and bid packages follow a familiar, recognized structure, (e.g. Construction Specification Institute or CSI format) and this helps you and the security integrator comprehend the overall project goals and vendor interactions.

The "second set of eyes" that a consultant provides to oversee the project can bring value, and can reduce risk to the end user. The consultant can add an objective view in selecting a product platform that best meets the customer's needs. However, be aware that all designers, whether consultant or security integrator, can only make recommendations based on the products they are familiar with, while most platforms share a great deal of common capabilities. It is impossible for any consultant to have knowledge of all of the products available in the industry, but most consultants are very familiar with several that provide "good, better and best" feature sets. Before working with a consultant, be aware of the boundaries of what a security consultant can provide, and consider that a fair portion of budget spent on consulting fees could be allocated to security products and services.

The output from a security consultant could be as basic as an "instruction list" for a particular project, including considerations of what components to use, placement and how to integrate them with a command center. The security consultant would not be responsible for the actual implementation, testing and maintenance of a system, but offers direction. If budget does not allow for a consultant on the project through the implementation and testing phases, you can work with a security integrator to review any items that may be unclear or vague as each instance appears.

// Option 3: Partner with a Security Integrator

The third option is to partner with a trusted security integrator to develop an overall physical security plan. This method can include benefits from both of the previous examples, resulting from direct and open dialog with the security integrator. The security vendor may provide site surveys and multiple system designs at little or no charge, and work with you to develop implementation phases that are in line with your budget constraints. This is where the “trusted” title gets put to the test - where it is appropriate and within the confines of the law, it is very beneficial to share budget constraints with the security integrator. If the integrator understands these concerns, standard procedures and culture, an ideal solution can be created. When the integrator has an idea of the neighborhood of the budget available to be spent, the solution can be tailored to include all required sub-systems, components and labor in order to implement the most effective system and maximize spend within that budget.

A security integrator may provide site surveys and design systems at little to no charge, and can develop implementation phases in line with your budget. If the integrator provided the design and is responsible for implementation, the integrator is accountable for project delivery, which can reduce overall risk for budget overruns.

A good integrator will not be interested in making this one sale; their goal is to partner with you to meet your long-term goals. Ultimately, you benefit from having a “second opinion” from the team that will perform the installation. Increased understanding of your expectations and operational procedures can reduce the overall risk for budget overruns on the project.

During implementation, you can reduce the likelihood of misunderstandings regarding system function and interoperability if you utilize a security integrator. If the integrator provided the design and is responsible for the implementation phase, the integrator will be held accountable for project delivery. Security integrators are experienced in providing these services consistently in a real-world, real-time environment, and are in the best position to understand the latest information regarding equipment and systems configurations.

Conclusion

The three most common approaches that you can take in the process of security design and implementation include: 1) Do it yourself, 2) Hire a consultant, and 3) Partner with a security integrator. Carefully considering all of the options against your unique situation will help you implement solutions that can provide additional reliability and potentially reduce operating costs and save time.

For more information on Security Design and Implementation, call 1.888.721.6612 or visit www.TycoIS.com.