

# ***The Need for Security Design Consulting***

by

Brian Gouin, PSP, CSC



(281) 494-1515  
bg@threatanalysis.com  
www.threatanalysis.com

Copyright © 2006  
Threat Analysis Group, LLC  
All Rights Reserved

You're a very busy hospital security manager. At 2 pm on one of your normal busy days, you receive a call from a man saying he represents a security consulting firm. He explains that one of the company's specialties is technical expertise in electronic security design. He asks if you have any upcoming projects or concerns and if you would like to meet with a company representative. Why should you not just politely say no and end the call? What could this firm do for you that you cannot do yourself? After all, you understand how to perform a risk assessment, have your hard earned certifications, and no one is more familiar with the electronic security needs of your facility than you are. While this may be true, the use of a security design consultant can be an extremely valuable tool to help you do your job.

While security management consultants deal with the full risk assessment and the entire security program, security design consultants deal with a specific and specialized piece of the assessment and security program, electronic security. Therefore, while the advantages to using a security management consultant are more 'big picture', such as budget verification or independent review, the advantages of using a security design consultant are more specific, dealing with issues like access, visual verification, detection, deterrence, and response. That is not to say that security design consultants do not deal with the total electronic security picture or how that fits into the overall security program. In fact, that is exactly what they do. In general, the services of a security design consultant fit into three categories: assessment, design and project management.

### **Assessment**

Assessment services are the services most commonly attempted by the security manager or security department. It is thought, correctly so, that you have the most knowledge about the overall security needs of the facility. However, having that knowledge does not necessarily mean you know what electronic security devices are required to deal with those security needs, where they should be placed to be most effective, how much they will cost, or how they should be integrated with all of the other facets of your security program. Let's say you have a visitor control issue that you have identified because of certain incidents or just by your observations of your facility. It is necessary to develop a needs assessment report outlining the type of electronic security devices that can help remedy the situation, where they should be located, how much they will cost and how will they be integrated with the rest of your security program such as guard force and existing monitoring capabilities. What do you do?

Unfortunately, what is done a lot of the time is some devices are identified to be placed in locations to deal with the perceived issue at that time. Many times these devices are merely extensions or additions to existing access control or CCTV systems which were not designed at the time to deal with your specific issue. It is easier and more cost effective to add to existing systems in the hope of resolving the problem rather than starting from scratch with a new approach. You may solicit the help of your existing

installation firm or even call in a new one to help you place new devices and add them to your existing system. They may even suggest different ideas than you had to deal with your specific issue. The problem is they are in the business of selling you equipment, not coming up with the best solution for your problem. That is not to say they are acting unethically, just that their reason for being there is different than your objective.

Let's say you make the correct decision and decide to evaluate the problem from scratch and figure out the exact needs of the facility, do you or members of your department have the specific expertise to make those decisions? Do you have a good understanding of all the functions and capabilities available in today's electronic security systems? Can you evaluate every reasonable option available to determine the best fit for your needs? Do you know how much these systems cost? If any of your answers to these questions is no, what do you do? You have the option of doing the best you can which may or may not be good enough, or finding a professional who can assist you in making the correct decisions when it comes to your electronic security needs.

A security design consultant has the expertise in evaluating the security needs of your facility and determines the best electronic security options to meet those needs. Additionally, the consultant has an understanding of how those options will integrate with all the other elements of your security program. The consultant can determine optimal device placement, deal with regulatory and code issues with the devices (especially with access control systems) and prioritize the importance of system functions and capabilities to make sure the ultimate equipment chosen matches the security needs. Finally, the consultant can provide realistic cost estimates so budgets can be set and no surprises come up during system procurement. All of these evaluations and recommendations from a needs assessment report that can be used to support your claim that a security need exists and should be addressed, ultimately helping you do your job even better.

### **System Design**

Now that you know what types of electronic security devices should go where and what their functions and capabilities should be, the necessary system needs to be designed. Let's say you have a complete and correct electronic security needs assessment showing all the correct device types, locations and functions. Do you have the expertise to know which products in the marketplace are the best fit for your needs? Do you know the correct things to look for in a product to determine if it fits your need? Do you know what things to avoid? Do you know how competitive the bidding would be based on those product choices? Probably not. This is no slight on you, the industry is just so complicated and fast changing that it would be impossible for you to keep up on all those issues and still do your job. What do you do as the security manager handling this project?

Unfortunately, a lot of the times you call a large installation firm (if they weren't already called in the assessment phase) that also advertise themselves as 'security consultants'. If you need specifications written for the project to go out to competitive bid, they may offer to write the specifications for you. And, to your good fortune for budget purposes, they will write the specifications for no charge. While you may think this is a bargain, it probably will cost more money in the long run. What typically happens is that company will write the specifications to make it extremely difficult and sometimes impossible for any products to be used other than their proprietary ones, making them the only company able to competitively bid the project. This creates two major problems: first is the equipment specified is more than likely not the best fit for your needs and second you will pay far more than you should for the installed system because it in effect becomes sole source.

What if, instead of having an installation firm write the specifications, you invite several reputable firms into your facility, explain to them what exactly you are looking for based on your needs assessment, and ask them to give you a proposal with products that will meet those needs and associated costs. Sound better? While it probably is better, it is still inherently flawed. Installation firms usually have certain manufacturers that they use the majority of the time either because they have a comfort level with that manufacturer or they have an actual agreement with that manufacturer to sell a certain amount of its equipment per month. What happens is the equipment is made to fit the needs even if it is not close to the best fit or the most cost effective option. Additionally, do you have the expertise to sift through the proposals to determine which equipment is the best fit for your needs?

A security design consultant is independent of any manufacturer or installation firm. Their product choices are based solely on the needs of the client. They match the product to the need rather than the need to the product. The consultant can prepare design specifications in two specific ways: for a Request for Proposal (RFP) or Invitation to Bid (ITB). A Request for Proposal describes in detail the system and equipment requirements as determined by the needs assessment and gives general criteria that the bidder must fulfill for their bid to be acceptable. The installation firm will then propose equipment to meet those needs and give a cost for the installation. The consultant will then evaluate all the proposals and make a recommendation as to which proposal best meets the needs of the client. An Invitation to Bid actually spells out the exact equipment that will be bid. The consultant will have already made those determinations based on expertise and industry best practices. The installation firm merely bids a cost for what is specified. In either case the product decisions are based solely on the needs of the facility and client rather than any other factors.

A note about using project architects to do the assessment and design work described above. This could be a good or bad thing. You need to ask some questions up front in order to make that determination. Does the architect use their own independent security consultant? If not, if they use an engineer or do it themselves, what expertise do they have in the assessment and design of electronic security systems?

Unfortunately you will find that some architects also use security installation companies to do this work for them. While they are getting the services for free, you are being charged. Additionally, you are getting far from the best system for your needs. This is certainly not always the case, there are a lot of excellent architects out there that either have the proper expertise or hire that expertise. You just need to ask the questions to make sure you are getting the best for your money.

### ***Project Management***

Once the procurement process is complete and an installation firm has been chosen to install the designed systems, someone must make sure the systems are installed per the specifications and industry best practices. It stands to reason that the best person to provide that oversight is the person who actually wrote the specifications. If the same firm who wrote the specifications is doing the work, that is not very reliable oversight. In many cases you as the security manager can do this project management oversight yourself or through your department with little difficulty. However, if the security design consultant has been involved in the project through the assessment and design phases, he is best able to evaluate the quality and thoroughness of the installation. Also, for more complicated systems and installations, having project management performed by someone with the technical expertise to understand what to look for in the oversight process is a great advantage.

So the next time you receive that phone call at 2pm on a busy day, perhaps you should consider hearing what they have to say. The consultants' job is not to upstage the security manager or in any way take away from the overall security program, but rather to enhance the capabilities of the security manager and the department in general by helping you do your job in the best manner possible. No one is expected to know everything, but you are expected to find people with the necessary knowledge when an issue arises. Take advantage of it.

### **About the Author**

Brian Gouin, PSP, CSC has over 17 years of experience in the security and fire protection field, first as the owner of a security installation company and then as an independent security design consultant with Threat Analysis Group. Brian has extensive training in system design from a vast number of manufacturers of electronic fire and security equipment. Brian is a member of the American Society for Industrial Security, the International Association of Professional Security Consultants, the National Fire Protection Association and the National Association of Chiefs of Police. Brian can be reached via email at [bg@threatanalysis.com](mailto:bg@threatanalysis.com) or via phone at (281) 494-1515.