Chapter 11

Security Measures: Deploying Physical Security

Karl F. Langhorst

In this chapter . . .

- Countermeasure Selection
- Creating Management Buy-In
- Countermeasure Implementation
- Auditing Effectiveness

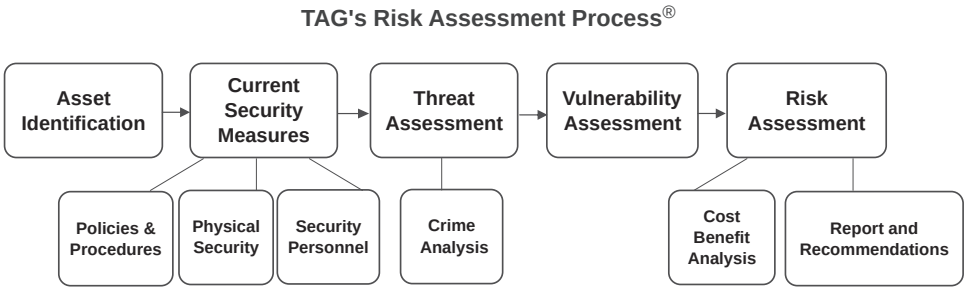

Figure 11-1.
Strategic Risk Assessment Process, Copyright ©2007 by Threat Analysis Group, LLC. Used by permission. Additional information available from Threat Analysis Group, LLC via www.threatanalysis.com.

Countermeasure Selection

Once a risk assessment has been completed and the report recommends that additional physical security measures are needed to help reduce the organization's exposure, it is time to decide what technology is best suited for the facility. If you are one of the organization's security decision makers, you are

undoubtedly inundated daily with mailings and phone calls from companies professing to have the latest and greatest security technology that will solve all of your organization's problems. While these vendors may have good equipment, it may not be the right equipment for the organization.

The first step a security decision maker should take during the selection phase of security equipment deployment is to decide what is to be accomplished. For example, if the security decision maker's goal is to install a camera system that can capture a license plate number of a car entering or leaving the parking lot of the facility at both day and night, the security decision maker must make sure that this criterion is specified to the vendor that is supplying a bid. That may seem like common sense, but many security equipment vendors will tell you that customers often fail to be specific enough about what they are trying to accomplish and overzealous, inexperienced salespeople don't ask. More often than not, when the technician comes to install the new equipment, he says, "I can install this but it's not going to do what you want it to." In these instances, the security decision maker just wasted valuable time and will more than likely have to start the bidding process over again and probably explain the misstep to management.

Be realistic in your assessment of the threat level to the assets in need of protection and the level of damage that could be sustained if in fact an intrusion does occur. If it is the organization's critical infrastructure in need of protection, security decision makers will certainly have more latitude in spending funds on needed equipment than if they are seeking to secure low-risk, noncritical assets. Rarely are security professionals employed at a company where they have an open checkbook to procure every piece of technology that they desire regardless of cost. More often than not, organizations make security decision makers justify every lock, camera, and alarm component that is being considered. The security decision maker who is not cost conscious during this process will be doing a disservice to the organization and the security program. Just because a certain technology is the latest and greatest does not necessarily make it the right choice for the application. A security professional knows that fiscal responsibility is part of his or her job description as well. Don't necessarily buy cheaply but do buy wisely. Security professionals manage their security budget as closely as they manage their personal finances. They will quickly get the respect of their supervisors and are more apt to get funding for future security expenditures if they are known to have fiscal restraint when making purchases.

A common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools.
—Douglas Adams

One of the best ways to determine what technology works for the organization or facility's environment and what does not is to see what other secu-

rity practitioners in the industry are using in their facilities. Hopefully, the security decision makers are already networking with these individuals and have established working relationships with them. If not, they are missing a chance to gather invaluable insight into how other companies are addressing some of the same security challenges faced by the security decision maker. Professional security and loss prevention associations, such as the American Society for Industrial Security—International, are ideal venues for networking with peers to both share and hear experiences that can benefit the organization. Obviously, confidential proprietary information should never be shared, but there is a wealth of knowledge that is not confidential that can be gained by interaction with security counterparts. Whenever possible, try to tour the actual facilities of other organizations to see what security measures they have implemented. Security professionals securing public facilities can be sure that others, including competitors, will be looking to see what you are doing to address security concerns. If the facility is not generally open to the public, ask your security counterpart if he or she would give a brief tour so that you can see what they are doing in the way of security. You probably will be pleasantly surprised by the willingness of other professionals in the industry who will provide valuable information to help you determine what equipment is right for your project. Don't let your pride in being a subject matter expert in every aspect of security get in the way of listening to other professionals in your industry who may have a wealth of information for you.

Security decision makers should avoid taking a myopic approach during the selection process of security technology. Usually, many different technologies are available to security decision makers, and thus they have many different ways to protect the asset in question. For example, would a simple single-cylinder deadbolt lock on a door and a motion detector with a local audible alarm satisfy the security requirements for the area you need to protect? Or does it require a more advanced technology, such as a proximity card access control system, with central station alarm monitoring capability? These questions can be answered by reviewing your threat assessment and vulnerability data so that you can formulate a logical, cost-effective solution. If the security solution proposals always reflect a "cost is not a factor" mindset, security decision makers will sooner or later be faced with some push back from management who become concerned about the cost. Remember, in most environments the Loss Prevention and Security departments are cost centers rather than profit centers, and the limited financial resources should be wisely spent.

When making a major purchasing decision on rolling out security hardware to multiple locations, a trip to a technology trade show would certainly be warranted. Large shows are held annually throughout the United States which offer security professionals the opportunity to view the latest and greatest in security technology. ASIS holds a yearly conference that features hundreds of exhibitors with displays of everything from locks to windows to alarms. Another major trade show is the International Security Conference (ISC),

which holds shows annually both on the West and East coasts of the country. Because of the extremely large number of exhibitors at these shows, security decision makers will probably spend a couple of days visiting with the different vendors, looking at their equipment and asking questions. This can be an overwhelming experience, and security decision makers can leave these trade shows with more questions than when they arrived if they have not prepared adequately. If, for example, you are looking for a digital video recorder (DVR) device to replace your existing VHS system at your facility, it would be advisable to prepare a checklist of the features you desire the system to have. It is not unrealistic to find 30 or 40 different manufacturers of digital recorders at these shows, and after looking at all of them the strength and weaknesses of each one can easily run together. By utilizing a checklist of what your specifications are, you can rate each unit to see how closely the product meets the organization's needs. After completing a tour of the show, you can then review the checklist for each vendor's DVR to narrow down which unit warrants a second look. By utilizing the methodology we have outlined, you will quickly be able to examine a wide variety of products in a short period of time, thereby reducing the length of your search process. Security decision makers do not have to become subject matter experts on every piece of security technology that they have in your facility, but they certainly should know how the product is supposed to function if they are going to recommend that the organization purchase it.

As previously mentioned, a lot of security equipment providers are trying to sell security decision makers their product. For example, if you are in the market for an alarm system, one decision you will be faced with is whether you want to purchase a proprietary alarm system or a nonproprietary system. Also, you will have to decide whether you want to lease the system or own it. The initial cost of getting a proprietary system and leasing it might appear attractive at the onset and could certainly save you the initial outlay of capital, but upon further examination this could tie you into a service provider that you are not happy with in the long term. By purchasing a nonproprietary system that can be serviced and monitored by several different providers, you are free to switch to a different company should the need arise. Additional consideration must be given to the type of alarms needed at the facility. Fire alarms are typically dictated by the local fire jurisdiction as to the extent and type of coverage required. Your organization's insurance provider may also have a say as to what type of equipment is required at the facility as well. Burglar alarm systems are typically not regulated by local authorities, except for alarm permit requirements, and therefore can be an area in which a lot of latitude is possible, allowing security vendors to oversell or even undersell.

When addressing security needs for multiple locations, it is very easy to fall into a "cookie-cutter" mentality. Busy security professionals can find themselves applying the same security solutions at every site they oversee. Standardization of equipment and how and where it is to be installed in itself is not

necessarily a bad thing. By using the same product throughout your facilities, members of the security department have the ability to familiarize themselves with the nuances of the equipment and are more adept at both utilizing and troubleshooting any problems with it. In addition, in environments where security personnel are not the only user of the security equipment, as is often the case in retail stores, security decision makers stand a much better chance of on-site, facility personnel using the equipment and taking ownership in maintaining its functionality if they are familiar with it. If facility personnel are frequently transferred from site to site, the last thing most of them want to do, or have the time for, is to learn how to operate a different type of security device whether it is CCTV, alarms, or even locks. Great savings in the purchase price of the equipment can also often be realized if security decision makers deal with the same supplier on a repetitive basis.

Quite often, security decision makers can fall into a trap that more is better, meaning the more expensive and state-of-the-art equipment they put into a location to harden the target, the better chance they have of preventing losses. Certainly, different layers of protection for a facility should be considered during the security assessment phase. But security professionals would be remiss if they did not propose realistic solutions to address the anticipated threat level. For example, as the security decision maker for your organization, you could propose to have a biometric access control reader on all of your exterior access doors at the corporate office if you so desire. And if your organization was in the business of dealing with government defense contracts, that type of system might not only be warranted but required by the government if you were to do business with them. However, if your organization did not handle top secret government contracts but rather was in the field of distributing car engine parts, would you be able to justify the additional expense and the necessity of a biometric access control system to management over the cost and effectiveness of a proximity card system? You might show management the costs for both systems and then make your recommendation to go with the less expensive but more applicable system for your facility. By taking this approach, you will demonstrate that you have the ability as a manager to make rational, cost-conscious decisions based on the best needs of your organization. This is not to suggest that as a security professional you should always recommend the least expensive alternative to address your security needs—far from it. You have an obligation to your organization and to yourself to always deliver a fair and honest analysis of any security issue you are asked to address. While this may not always be the popular approach, it is the approach that in the long term will earn you the most respect.

Another critical component during the selection process of any security hardware for the facility is service. You can select the most user friendly, cost-effective security product that you were able to find, but sooner or later, regardless of its dependability, it will break and need service. And when it does break, you need to have a good, reliable provider in place. Otherwise you might have

a nice piece of high-tech security equipment that has more value as a door stop than a door lock. When considering making a purchase, the security sales representative for that product will tell you how good their service is and how they are available to you 24 hours a day if need be. That type of verbiage looks good in a sales brochure or in a PowerPoint presentation, but is it true? It is incumbent upon the security decision maker to find out. The old adage of "Let the buyer beware" certainly applies here. You should first ask for references in your industry of those who are using the product. Then you should call those references. Never assume that just because someone is listed as a reference for a vendor they are not going to give you a less than positive opinion of them. Sometimes vendors list references who have not even approved use of their name on such a list. If you run across this while researching the reference list, this should be an immediate red flag to you. But don't just stop at calling the list the vendor has provided to you. Go back to that group of peers in your industry that was mentioned earlier. They can serve as an invaluable wealth of information about service success stories, as well as dilemmas, involving equipment you are considering purchasing. And if they are not currently using the equipment you are interested in purchasing, odds are they know someone who is. Many questions need to be asked of these professionals to see how closely their answers coincide with those given to you by your sales representative. Have they had to call for service to the product in question on weekends, holidays, and late at night before? If so, how quick was the response time to their call, and how knowledgeable and well equipped with spare parts was the technician that responded to the location to complete the repair? After gathering all of that information, you should personally give the company a service test. Why not try calling that 24-hour service number at 2 A.M. to see if you get a live person as they promised in their sales literature? As a security decision maker, you will be inundated by many companies that are going to compete for your business. In many cases, they will be selling product that closely resembles each other in both performance and pricing. What really sets these products apart in many instances is the service aspect of the company. One of the most frustrating things for an end user of security products is to have a high-priced piece of technology fail and then be informed that the service technician will not be available for 72 hours. If you needed the technology badly enough in the first place to spend your organization's capital to purchase it, why should you be expected to wait three days to have it repaired? Many security equipment vendors will give a company the opportunity to test their product on a "try buy" basis for a short period of time; 30 to 60 days, for example. In these cases, you agree to test the product and either return it or purchase it at the end of the prearranged time period. While this is not a realistic expectation when dealing with something as complex and permanent as a fire system, for example, it is feasible with a digital recorder, CCTV camera, or maybe even a locking device. What better way to see if the equipment is what you really want in your facility and if it performs to your expectations. And in

the event of an equipment problem, you get the opportunity to see their service personnel in action. Lastly, when it comes to service, if during the purchase phase of your equipment procurement you have difficulty contacting your salesperson and he or she does not return phone calls or show up at appointments in a timely manner, what type of service do you expect you will receive when you have difficulty with the equipment you are trying to purchase?

Finally, before deciding on which vendor you want to purchase your equipment from, you should make sure the company you are going to do business with will be there in the future to service your needs. Every year more and more companies enter into the market to sell their newly developed security hardware devices. Most of these companies will do anything to get your business, including giving you rock-bottom pricing. Unfortunately, while their product may be very good, the management of the company may not be. In today's economic market there are never any guarantees that any company, regardless of its length of operation, will be around tomorrow. But there are signs that you can look for that may indicate a lack of stability within the company. One sign is the continued promise from a salesperson that her company has new technology that is "just about to be released" that is exactly what you need for your application. Inevitably, those promised release dates continue to be pushed back. This could be a warning sign reflecting anything from the company having difficulty obtaining the necessary capital to fund the project to a turnover in engineering personnel to problems developing the technology itself.

Another possible red flag of looming difficulty with the company is a continual change in sales representatives or administrative personnel. Quality sales personnel are usually in high demand and therefore will not stay with a company long if they do not feel it is stable. A thorough examination of any company should also include determining if the sale of security technology is even their primary business. During the initial frenzy of the digital video recorder era, there were many start-up companies selling their latest technology. Many of the companies had little if any background in the security industry. While their equipment may have been sound from both a hardware and software point of view, quite often it was not well thought out from the perspective of the intended end user, a security professional. In addition, some hardware developed by companies with little security insight might be easily defeated by an intruder due to lack of knowledge by the designers of the types of threat their product might be vulnerable to. Truly the selection of the company you decide on as your equipment provider can be as important as the equipment itself.

Creating Management Buy-In

Once you have cleared the first hurdle of deciding what equipment you want to purchase, the next hurdle, and sometimes the most difficult one, is convincing management that you need it. Depending on the type of facility you are

responsible for protecting, this can be a relatively easy task or a difficult one. Some facilities, such as nuclear facilities, are highly regulated and therefore are mandated to have certain security features in place. On the other end of the spectrum, if you are responsible for protecting a chain of convenience stores, which typically have little government oversight as it relates to security, you might have a more difficult time getting all of your security recommendations approved that require capital implemented, even though this can be an inherently dangerous work environment. Hopefully, you have already established a strong working relationship with senior management, and as such they respect your decision-making process and recommendations. This is not to say that this support will gain you instantaneous approval for your proposed expenditures, but it will help lay the groundwork for a more receptive audience.

One of the first tools you should utilize in your equipment purchase presentation to management is the risk model that you have compiled. It is of the utmost importance that they understand that you have done your homework before bringing this proposal to them for their consideration. Owing to time constraints, you more than likely will not, and probably should not, review the entire risk analysis model that you have developed for the site but rather present a top-level briefing of the key points of your analysis. At the end of your presentation you can provide a more in-depth response on your analysis if questions are offered to you. Keep in mind that these risk analysis models that you have built, if done properly, will not only be useful in the design and equipment procurement phase of your project but may prove useful in the future to defend your company against civil claims of negligence arising from criminal acts that might occur at your facility. As part of your briefing to management, you should include any relevant internal crime statistics, especially if this is a preexisting site where you may have such data readily available. Many organizations that do not have facility security personnel at every facility struggle with accurately tracking criminal acts that occur on their premises. Quite often they only find out about such incidents when they are contacted by law enforcement, or even worse when they are served with notice of pending litigation from the plaintiff's attorney. To help counter this problem of the failure to report relevant incidents, your security department should make sure that they have provided an effective and nonlabor-intensive means in which facility management can do so. Several different methodologies exist that might be suitable for your organization. A call-in phone line to a staffed data center might be an option for a large company whereby operators key in the information to a database as it is relayed to them by the reporting manager. For companies with an advanced intranet network, an online report might be a viable option that can be completed and instantly e-mailed to the appropriate security personnel 24 hours a day with the push of a button. Even a basic pen and paper report completed by management and faxed to the security department can be an effective means of documentation if that is all that is available. Regardless of the methodology used, it is important that constant communication is ini-

tiated by security department personnel to the appropriate operations staff of the need to report criminal acts committed on their premises.

Organizations should not rely solely on their internal databases to determine what crime is occurring at their facilities. It is a good idea to check local law enforcement records if they are available to determine the crime statistics for your locations. A note of caution should always be observed, however, when you are strictly using police records for your site security recommendations. In the case of large office complexes or shopping centers, law enforcement officers will sometimes just list the address of the largest facility in the immediate area as the offense location. This is especially true at shopping centers made up of individual retailers that share common parking areas. The end result might be that criminal offenses are recorded as having occurred at your facility when in fact they occurred at a neighboring business. In addition, certain research firms can provide in-depth crime research of law enforcement records reflecting crimes committed in or around your property. Some of these companies take the time to individually review each criminal offense that is listed in police files as having occurred at your location. The particulars of the offenses can be communicated to you (ex: time of offense), and possible patterns of crime may be discerned that may be especially useful to you in the deployment of your security resources. These services can be especially useful in areas where you do not have on-site security department staff to perform an in-person site assessment of the property in question and to consult with local law enforcement officials about area crime statistics.

Documentation, including prior premise liability litigation specific to the site under consideration, can most definitely have a positive impact on the approval process if you can tie the security equipment you are proposing to the future reduction of exposure in liability claims of the nature your company has experienced before. During your presentation, it sometimes helps to work in a "war story" if applicable about how the technology under consideration was responsible for either deterring or detecting criminal activity. If you have first-hand knowledge of how the equipment has performed in an incident at a previous employer, at another one of your facilities, or perhaps even at a competitor's location, this could be an opportune time to let management see the real-life applicability of the equipment. Don't neglect to utilize the information you hopefully have already gleaned from competitors on the type of equipment they use if you feel it would be beneficial in supporting your proposal. If you are in a business that is under intense public scrutiny, such as a retail establishment or public transportation company, it is especially important to note that your customer base has a certain expectation of security while on your premises or utilizing your services. Whether or not the expectation is a realistic one is often debatable, but the indisputable fact is that they do have that expectation to varying degrees. For example, if your competitor has better lighting than you do in his parking lot, you will inevitably hear about it from your customers and quite possibly your employees. Damage to your public

image due to security lapses, especially since the September 11 attacks, is a definite concern that needs to be considered during both the design and approval process involving security equipment.

Increasing the value of the security equipment you have proposed to your organization is another way to get management to buy in to the expenditure. For example, if you are trying to get a new CCTV system installed at a facility, look beyond the security applications of the system. Examine other ways the cameras can add value to the organization. For example, if you have a facility that is open to the public, are there any areas of the building in which you have an inordinate number of slip and fall claims by customers? If there are, propose putting a camera there to help capture some of those incidents to see if they're indeed legitimate claims or fraudulent ones. In today's litigious society, it would only take a couple of fraudulent claims that could be denied using CCTV footage of the incidents to pay for the proposed CCTV system. You could also make camera surveillance footage available to distribution or operations management if cameras were located in areas in which they wanted to measure worker productivity. Before making your final sales pitch to whomever in your organization is responsible for the equipment expenditure approval process, you should reach out to your counterparts in other departments to see in what way the equipment you are proposing can be of benefit to them. By doing this in advance and including their positive feedback in your presentation, you are building value for the proposed equipment and increasing the likelihood of getting your expenditure approved.

Probably the most important part of the proposal process is how you make your presentation. More often than not, depending on your position, your presentation will be before the management of your organization. It is extremely important for the success of your proposal, and quite possibly your career, that you deliver the proposal in clear, concise terms and keep the presentation as brief as possible. Never embellish on the performance or the need of the equipment. That tactic will come back to haunt you. Once your presentation is over, be prepared to answer questions with short answers if at all possible. The managers you are dealing with will more than likely have numerous other matters to address besides your proposal and will generally appreciate your brevity.

And finally understand that you will not win every battle. There will be times when you will be told no to your recommendations. While this may be hard to take personally, if you have taken all of the steps you believe necessary to educate your organization's management on the need for the proposed equipment, then you have done your job. If repeated security expenditures you propose are denied over a period of time, then you should consult with your manager to determine what, if anything, you could do differently in your preparation process or presentations that might have a more positive effect on the outcome. As importantly, you need to reaffirm that your security philosophy parallels that of the organization for whom you work.

Countermeasure Implementation

The installation phase of your project will now begin, assuming management has approved your proposal for the expenditure of monies for security equipment. Before delivery of the equipment, every site should have an on-site visit from a member of the security department to make sure the facility is ready for installation of the equipment. Once the equipment arrives, make sure your vendor secures the equipment in a safe place over the course of the install. What could be more embarrassing to explain to your management than that the security equipment was stolen? Even after the equipment is on site, it is imperative that a knowledgeable security representative monitor the progress of the equipment's installation to ensure that it is being installed according to bid and meets your organization's expectations. Those who have been involved in the construction of any facility will tell you that it is an evolving process. A blueprint may reflect one thing, but during the actual building of the structure the doors, windows, and even walls can be moved or modified based on revised needs. Whenever this happens, it is imperative that the security needs are reassessed to determine what changes, if any, need to be made in the equipment specifications and installation. To leave this task in the hands of a vendor can lead to ineffective or improper installation of security equipment, and subsequently it could cost more to correct. The old adage of "inspect what you expect" has never been more relevant. This is not micromanaging; it is simply making sure that the resources security decision makers have been entrusted with are being utilized in the most effective manner. In addition, the sooner a needed change in equipment type or location is detected during the construction process, usually the easier it is to effect this change.

A wise security decision maker will quickly develop a partnership with his organization's construction department to enlist their help in monitoring the correct installation of security equipment. Security personnel should attend on-site construction meetings with all of the other vendors during the building process to make sure their needs are being addressed and to help educate the vendors on what those needs are. Communication with the contractor overseeing the entire construction process is also critical. For example, when installing a CCTV system, you probably will want to have it on a dedicated power circuit. This in turn should be connected to an uninterrupted power supply (UPS). There is no more appropriate person than the security representative to ensure that this is communicated to the construction superintendent and the electrical contractor. By building a good rapport with these individuals and letting them know what your needs are, security decision makers are much more likely to have those needs addressed properly and in a timely manner.

There are many competing interests during the construction of a facility. If you or a member of your staff are actively involved during the construction

process and interact in a positive manner with the construction personnel, you stand a much better chance of developing a long-lasting partnership with them. Another benefit of this interactive approach is that you might possibly develop another "set of eyes" to spot any security-related issues on future building projects. At the end of the installation of the security equipment, it is beneficial, especially on large projects, that you develop a checklist for the security vendor to ensure they have completed the project per your expectations. For example, if you are having an alarm system installed, has the technician walked the system to ensure the motion detectors are providing adequate coverage of the area in need of protection? If a panic or duress button has been installed, has it been tested to make sure that the central monitoring station has received the signal? What could be worse than someone working at your facility pushing a button with the expectation that it will summon help and it does not work. Nothing will make security installers more accountable for their work than having them personally sign off on a checklist that they have completed the installation process in the specific manner that you have previously outlined to them.

Once the installation phase of the project is completed, the next step is to make sure that the on-site staff knows how to operate the equipment and utilizes it in the intended manner. Many companies include training sessions on their equipment in the purchase price. The training should be utilized to make sure that the end users of the technology understand all of its features that can assist them in protecting the facility and its assets. This is especially important at locations where there are no on-site security personnel and facility personnel have direct responsibility for utilizing the security equipment. If the security decision maker expects to get buy-in from facility personnel and management to utilize the security equipment that has been put in place, then it only makes sense that the management is trained on how to use it. Management should also be educated as to why the equipment was installed and how it helps them. You do not want to leave the facility personnel and management with the impression that this is just another item they have to take care of or watch over because the corporate office says to. They need to understand the value of the equipment. Much as you had to sell management on the need for the equipment, you now have to sell the end user as well; otherwise your efforts will have been in vain.

Maybe you have installed an alarm system at a facility that records data on a printer in the facility manager's office every time an exit door alarm is deactivated. The facility manager needs to check this log daily to determine if possibly someone has gotten the disarming code and is covertly removing equipment or product from the facility via this exit. Or, for example, you might have an advanced digital CCTV system that the facility manager can use to review not only security concerns but worker safety and productivity issues as well. The more value you can convey to the facility manager regarding the security equipment you provided them, the more likely they are to use it. Facility

personnel should also be convinced of the importance of immediately reporting to security any equipment that is malfunctioning so that repairs can be affected. Although it might be somewhat burdensome for a security department to have to ensure that repairs of equipment are being addressed in a timely manner by security product vendors, the positive result in following this approach is that the repairs can be tracked more efficiently and they will more than likely be completed in a timelier manner given the more focused oversight. In addition, it is also easier for security decision makers to more quickly detect trends in like equipment failures at multiple facilities. This information can then be relayed to the security product vendor to determine whether there is a need to modify existing equipment at other facilities before it encounters the same difficulties. Information of this type would be especially useful if additional equipment was being considered for future purchase from the manufacturer whose equipment was failing.

Auditing Effectiveness

To further ensure that the security equipment that has been installed is being utilized as intended, an audit process should be implemented. Security department personnel should regularly check to make sure the equipment is functional and that it is being used according to the organization's standards. For example, if you have a facility that has a digital CCTV system that you have set up to monitor alarms in high-risk areas at certain times of the day, you more than likely have implemented guidelines that require the facility personnel to regularly check to see if alarms have been generated on the system. As with any other required security standard, simply setting the standard and communicating it to organizational personnel does not ensure compliance. Auditing the use of security equipment greatly increases the likelihood that the equipment is being used to the organization's standards.

Yet auditing just for the sake of auditing can be a waste of time if the security department audits are not backed by the organization's management and operations team. Too often in the corporate culture, audits are conducted by security personnel and operations responds with "lip-service" promising to correct the problems found in the audit, but rarely following through with those promises. Audits without management support may identify the problems, but rarely do they correct them. This is not to say that security must always go in with a "big stick" or with an "I got you" mentality when conducting audits. To the contrary, security personnel should continually strive to be viewed as part of the team. Whenever possible, audits should be put into the context of an opportunity to educate management on existing security programs.

Establishing good rapport with facility management is of the utmost importance if a security program is to be effective. By showing facility management the usefulness and effectiveness of the security tools that have been provided

to them, there is a much better chance that you will get their buy-in and compliance with security programs. Crucial elements of any effective security program are buy-in from the end user and support from organizational and facility management not only for the program itself, but also for the appropriate disciplinary action for those who continue to resist adhering to established security practices and protocols. Hopefully, this will not happen very frequently in any organization, but it will inevitably occur, and when it does it needs to be addressed rather than overlooked if the security program is to remain viable. More often than not, if a security decision maker has formulated a program that has been shown to be effective and has partnered with the end user of their services and equipment, those individuals will be reaching out to them for assistance and to discuss security issues. What better compliment to a security program if, for example, you oversee security at multiple facilities and the facility managers at one of those facilities calls to ask you to get the same state-of-the-art CCTV system installed at his site because he has heard and seen what a great tool it has been for the facility managers of the other locations that have the system. This type of favorable response is a strong indicator that your security program and the technology you are selecting is a value to your company.

In most organizations, justifying the need and expense of physical security equipment will always be a continuous effort. Success in getting approval for capital for these projects will hinge on the security decision maker's expertise in selecting the right equipment and provider as well as in justifying the need for the expenditure. To help gain future approval of projects, it is very important that security decision makers document and share their success stories with organizational management responsible for making the decisions on future purchases. In this way, management will see the positive end results of such expenditures, thereby greatly increasing the possibility that the security decision maker's future proposals will gain at least a hearing.