How to Develop and Implement a Security Master Plan

How to Develop and Implement a Security Master Plan

TIMOTHY D. GILES

CRC Press
Taylor & Francis Group
Boca Raton London New York

CRC Press is an imprint of the
Taylor & Francis Group, an **informa** business

Auerbach Publications
Taylor & Francis Group
6000 Broken Sound Parkway NW, Suite 300
Boca Raton, FL 33487-2742

Auerbach is an imprint of Taylor & Francis Group, an Informa business

No claim to original U.S. Government works
Printed in the United States of America on acid-free paper
10 9 8 7 6 5 4 3 2 1

International Standard Book Number-13: 978-1-4200-8625-6 (Hardcover)

Visit the Taylor & Francis Web site at
http://www.taylorandfrancis.com

and the Auerbach Web site at
http://www.auerbach-publications.com

This book is dedicated to my wife, Linda, who has encouraged me to undertake this task and supported me through this process as well as my children, Amy and Kelly, who have cheered me on to complete this work. It is also dedicated to the many security professionals that I have worked with over the years as a tribute to their unselfishness in sharing their knowledge and skills with me. I hope my sharing of this information will repay them in some small way.

CONTENTS

AUTHOR PAGE

Tim Giles is the president of Risk/Security Management & Consulting. Prior to going into business for himself, Mr. Giles was the managing director of security services for Kroll Associates in Atlanta for 2.5 years. Before that, he served as director of security for North America at IBM where he was the executive responsible for the firm's security operations for all of the United States and Canada until he retired after 31 years of service. Mr. Giles has also worked in IBM's Latin America operations as the director of security for two years and spent three years living and working in the Asia Pacific Region of IBM's security operations as the area security manager. While in Asia he was responsible for the security planning for IBM during the 1988 Olympics in Seoul, South Korea. In previous careers at IBM, Mr. Giles worked in manufacturing and engineering positions in IBM's semiconductor operations.

Mr. Giles was board certified in security management as a Certified Protection Professional by ASIS International in 1997 and as a Physical Security Professional in 2007. He was selected as the Security Director of the Year in 1997 by *Access Control & Security Systems Integration* magazine.

During his more than 25 years in security, he has worked in all aspects of physical security, information protection, investigation, crisis management, emergency planning and response, disaster contingency planning as well as managing major projects in most of these areas. He has also become very accomplished in utilizing all aspects of security technology. He spent 18 years working in the corporate security arena and has spent the following years working as a security consultant. He is also a licensed private investigator.

Mr. Giles is also an accomplished lecturer; he has conducted sessions in the following areas:

- Workplace violence protection programs
- Emergency planning and response
- Crisis management
- Security master planning
- Protection guidelines for today's business person
- Personal and travel security
- Establishing a global security program

Mr. Giles is an active member of ASIS International; he is the host committee chairman for the 2008 Seminar & Exhibits in Atlanta and is a past chairman of the Greater Atlanta Chapter.

INTRODUCTION

For several years I have conducted an education session at the annual ASIS International Seminar and Exhibits on the subject of "Developing a Security Master Plan." Although the sessions were well received, I have been contacted on a number of occasions asking for more insight into and information on the process of how to implement the Security Master Plan. As a result of these inquiries I decided to write this book on the entire process. You may find as you study these writings that I periodically venture away from the primary topic to expand on my own personal beliefs or philosophies in different areas. I try not to indulge in this practice too frequently; however, I do believe it is important to let you know where I am coming from in certain arenas. I doubt that every reader will agree with me on all of my narratives, but that is what makes the security industry so interesting. I hope you find the book interesting and informative and I wish you success as you pursue this endeavor.

This process varies depending on the size of the business or institution. A multilocation or multifacet business (e.g., manufacturing, research, office complexes, warehouses) or an international business will require more work than a single-site business or institution such as a hospital, for instance. However, even a single-location business or institution will have a variety of environments that will need to be addressed (e.g., emergency room, infant care, psychological center). It is very important to make sure that security is being implemented appropriately for each particular environment. It will also vary based on the way the security organization is structured and staffed. For example, if you have a security force consisting only of contract guards and no internal security professional, then you will need to determine if the contract for security includes all of the needed skills such as investigative, education and awareness, and executive protection. If these skills are not part of the contract then you will need to determine if that is appropriate as a part of your recommendations.

You will need to decide how many and which locations will need to be reviewed in order to properly define the current status of security within the business and to develop your recommendation for changes. This does not mean you must review every location of a multilocation business but you do need to look at all variations of the business. If the business, has its own research and development, manufacturing, retail, sales offices, and

warehouses in multiple locations, then you should work with the management team to determine which of these locations should be part of the review. You should look at a minimum of two locations of each type, and if you find a wide divergence of how security is implemented between them, then you should discuss adding additional locations to the review with the client. If you are dealing with an international firm, it is critical that you evaluate the risks in each of the countries. The risks that exist in the United States are not the same as the risks in many other countries; therefore, the security requirements will differ as well. For example, in my opinion, workplace violence is basically a U.S. phenomenon; therefore, it would not be appropriate to implement security programs directed at deterring this issue in other countries where this is not a risk.

SECURITY MASTER PLAN PROCESS

Definition:

A Security Master Plan is a document that delineates the organization's security philosophies, strategies, goals, programs, and processes. It is used to guide the organization's development and direction in these areas in a manner that is consistent with the company's overall business plan. It also provides a detailed outline of the risks and the mitigation plans for them in a way that creates a five-year business plan.

INTENT OF THE MASTER PLAN

It is my intent to show you how to construct a Security Master Plan, which will aid you or your client in gaining "buy in" from the executive management team on the direction of the program and the necessary budget to support it. I think most of us know that in the real world, even though clients have an approved budget for the out years, that does not mean that they will actually get all that money when it comes time for it to be approved and released. However, by having a five-year plan that has been agreed to by the management team, they have a much better chance of getting that money released, and even if they do not get it all in the year that they wanted it, that only means that it slips out to the next year as opposed to being lost completely.

BEGINNING THE PROCESS

I have written this book with the idea that a security consultant is performing the work; however, there will be times when I address items to the "in-house" chief security officer (CSO) or director of security. I will attempt to make it clear when doing so. Of course, this work can also be performed by the in-house security professional in lieu of utilizing a security consultant; however, I will point out many areas where this is a less effective process. When these areas are addressed, I will provide the in-house person with some ideas on how to compensate for that concern, and as a result, I feel that they will still be able to significantly benefit from this work. When you begin this process of developing a Security Master Plan, the first step is to request information from the client. If this is performed by someone internal to the operations, you will still need to compile this information. This information will give you the opportunity to do some preparation prior to being onsite and it will give you some insight into the operation to be reviewed. Once you receive the information, you should analyze it in detail. For example, if they send you two years' worth of internal incident data but no trend analysis, then you should do the trend analysis yourself to see just what the incident data tells you. You should also review the reports for quality and consistency as well. The information I usually request includes the following:

- General background information on the company
- An organizational chart for the management of the facility
- A copy of the post orders
- A copy of the site security manual
- Blueprints of the facilities to be reviewed
- Copies of any security-related procedures or practices, including information protection
- Copies of incident reports for the past two years
- Copies of any incident summary or analysis data
- Copies of any crime statistic data on hand
- A copy of the contract guard contract, if applicable
- A copy of any other security-related contracts, such as confidential destruction
- The current staffing of the security organization by rank
- A listing of any cash operation onsite including how much cash is kept on hand
- A listing of any precious metals stored onsite and their value
- Any unique security-related issues you should be aware of
- The location of any high-security areas onsite and why they are so considered
- Security system information, brand name, and model or level
- Type of lock and key system(s) in use at the facilities

Several different aspects of this process will require you to interview some of the top executives of the company. Although these areas of questions will be defined in each of the appropriate sections, it is important that you combine areas of questions and limit the number of times you need to interview the executives. Preferably you will cover all of the questions in only one interview of each of them, because you will want to avoid giving the impression that you do not value their time.

1

The Business of Security

WHY SHOULD YOU DEVELOP A SECURITY MASTER PLAN?

As a security consultant your responsibility with this process is to utilize the information in this book to help the chief security officer (CSO) or director of security gain executive management support and improve their potential for obtaining the necessary budget funding for their programs. It will instruct you and them in the proper process for building a Security Master Plan and its components, which will document the security strategies of their business or institution both for now and more importantly for the future. The end product of this will enable them to gain the support of the executive management team, and when effectively utilized, it will become their preamble to gaining the necessary budget funds to implement their security program. If the client you are working with does not have an in-house security professional, then it is the consultant's responsibility to accomplish these goals.

An important aspect of this development process is to make sure their security strategies are linked to the strategies of the business so you can ensure they are moving their programs forward in unison with the business. By doing this you will demonstrate to executive management that the security operation is no longer just a business expense but it is an integral part of the business and contributes to the success of the business.

FIGURE 1.1 Executives are often focused on numbers and bottom-line results in addition to a host of other day-to-day issues. As such, they often do not recognize how the security department can bring value to the business as a whole.

It is important to understand that although we security professionals are focused on the many diverse risks that face our businesses and people, the executives who manage that business are not (see Figure 1.1). They have many issues that occupy their time and thoughts on a daily basis. That is not to say that they do not care about these issues; they absolutely do. In fact, I have never met an executive who was not extremely concerned about any issue that might affect the employees or the business. I simply wish to point out that they are not as involved in them as we are. This process is the vehicle that will provide you the opportunity to bring these issues to the management team's attention through a business process and give you the platform for gaining the support the security function needs to effectively manage the risks that confront the business or institution.

Building a Security Master Plan will differ considerably from just conducting a site security assessment because you will not only need to identify the good and bad of the current programs, you will also need to help develop the corrective actions and long-term strategies. This would normally require that the person working on this master plan process have extensive knowledge and experience in all aspects of security programs and technology. However, this book will provide the necessary guidance and information to help compensate for a lack of experience or knowledge and assist you to develop the plan. The process defined in this book is

designed to be utilized by an outside professional, a security consultant, as opposed to being performed by someone who works within the current security organization. However, it can also be performed by an internal professional, but in my opinion, you will find that with some areas of the process it will be difficult for an internal person to be completely objective. Areas such as defining the current skills and knowledge of the security organization will be especially difficult for them. Also, although I sometimes implement this process on my own, you have the option of supplementing your skills with others who may be more skilled in certain areas than you are. I find this team approach to be an effective way to achieve the end result.

ENGAGING THE STAKEHOLDERS

It will also be important to put together a group of functional representatives from across the business to provide advice on where they believe there are currently areas that need change or improvements and how they perceive the recommended changes affecting the day-to-day operations of the business. Typically these representatives would be from the following groups: facilities or engineering, human resources, information technology, manufacturing, research and development, and administration, as appropriate to the specific client. If the business has union workers you may want to have a union representative in this group as well. The exact makeup of the group will depend on the business or institution that is being evaluated. This group, referred to as "stakeholders," is the representative of all of the internal and possibly some external organizations that would be affected by changes to the security technology, policies, and practices. By involving this group in the process from the beginning you will gain cross-functional support for implementing the necessary changes that will come out of the process. Of course, you may also encounter some resistance to some of the recommendations for change, but this will give the CSO or director of security or you the opportunity to address these issues early on, and even if they are not fully resolved, you will at least have knowledge of what issues need to be addressed with the executives when it is time to meet with them.

I would add that in the corporate world it is commonplace today for many functions to hire outside consultants to do assessments of their operations and provide an unbiased view of what should be changed or improved. This is almost the standard with some functions such as the

finance and the information technology (IT) organizations. It is interesting to note that while there has been some change in recent years, typically the security community does not take advantage of this kind of independent review nearly as much as the other functions. I believe this is a change whose time has come, not just because I am a security consultant myself, but because as a community we need to draw on the skills and knowledge of the experts within our profession more effectively and more consistently than ever before. As someone who has been a security director, I understand how difficult it is to just manage the day-to-day operations of your business and how little time there is to keep abreast of the fast paced changes that engulf our industry. By having a consultant come in to look at the operation with a new set of eyes, you can gain immeasurable insight into what changes you should be focused on.

Although many of today's chief security officers or directors of security have a good insight into the technological changes that affect the security world and have their own ideas as to what direction they believe their business will take relative to these technologies, I have found that only some of them have actually documented this direction in a sound business plan and shared it with their management. For example, many of the CSOs or directors of security that I have dealt with over the years who were utilizing magnetic stripe badges had never talked to their management team about migrating to proximity badges until they were in the process of requesting the monies to implement that change. In today's security world I believe you would not find many organizations that have a documented migration plan to move from proximity badges to utilizing either smart card or biometric (or both) technologies for their badges. Just as you would not find many of them that have a documented plan to implement intelligent closed circuit television (CCTV) software for their camera systems. However, I think if you asked the CSOs or directors of security, you would find that all of them believe they will move in these directions within the next few years. The Security Master Plan process will provide them with the right vehicle to correct this situation.

WHAT SHOULD YOUR SECURITY PHILOSOPHIES BE?

This area is to be reviewed by the security consultant; however, the development of the philosophies should be done by the in-house security organization. If there is no in-house security organization then the consultant should attempt to work with the in-house person who manages

the security contract to develop the appropriate philosophies for them to follow. First, I believe that the philosophies of the security organization should reflect the culture of their overall business. Next, they should reflect the leader of the security organization's business beliefs and, to some extent, personal beliefs and character. These philosophies are the basis upon which the security program is built. For example, some of the beliefs that I have personally used include the following:

- "Respect for the individual." This respect should be for each and every individual, including the ones who are believed to be violating your security policies and procedures.
- "Excellent service to the customer." This applies to both internal and external customers and at every level of the security organization.
- "Excellence as a way of life." Every action should always be done to the best of one's ability.
- "Managers and supervisors must lead by example." This is a critical aspect of projecting how all employees should act. "Do as I say, not as I do" will never work.
- "We should always be a good corporate citizen." For the security organization this is reflected in the way you deal with and support the many public organizations you interface with such as law enforcement, fire departments, and rescue services.

Of course, these are only examples of some of the philosophies I have used. This is truly a personal choice for the person who is in charge of the security organization. It is doubtful that you will encounter many CSOs or directors of security who have actually written their philosophies down and shared them with their staff. I firmly believe it is an exercise worth undertaking and that it can be a guide for the entire security organization. In many cases the company will have written philosophies or principles that they publish for all employees. If they do, then I would recommend to the CSOs or directors of security that they expand on those to help the security organization understand how they should be reflected in the day-to-day operation by the security staff, and they should also add some of their own philosophies to them and in support of them. If the organization utilizes contract security officers, it is very important that they are also made aware of the organization's philosophies. It may be necessary that they or the contract manager translate these into statements that reflect how these philosophies actually affect the day-to-day duties of the officers as well. This is usually done through the post orders; however, they may need to be elaborated to get the desired result.

CONTRACT SECURITY RELATIONSHIP

It is exceedingly important for the organization to have a "partner" type of relationship with the contract security force. This can be a delicate situation because the client does not want them to believe they are "employees" of the organization, but they should want them to see themselves as an integral part of the team. This is typically achieved by making sure the chain of command is always used when dealing with the security force. It is also critical that their own management, both onsite and offsite, have discussions with them on occasion about maintaining the right relationship with the "client." It will be very important for you, the consultant, to determine if this relationship is sound and appropriate. A common development in this environment is that you will see one of the lead people of the contract force begin to develop a personal relationship with some of the lead people on the in-house security or other staff. Over time this can manifest itself into problems where they begin acting as if they are an employee of the organization, instead of the contract force. Likewise, the organization begins to treat them more like an employee and even gives them more power in the relationship than they should have. Whenever this situation develops, the only effective way I have found to correct it is for that person to be taken off of that site.

WHAT SHOULD YOUR SECURITY STRATEGIES BE?

Before you begin the process of defining or redefining the security organizations strategies, you must first gain an understanding of the strategies of their business. You do this by interviewing the appropriate executives of the company: the CFO, COO, and so on. You need to know for the next five years:

- What growth do they anticipate?
- Do they expect any product or service changes?
- Is the expansion or reduction limited to the existing facilities or will new ones be added?
- Do they expect any overseas expansions or mergers?
- Are there any major layoffs or outsourcing activities planned?

Some of this information will be considered to be highly confidential, especially any mergers or layoff activity, but you need to understand these directional moves if you are to plan how they will deal with them from a

security standpoint. It is not necessary for you to know all of the details; for example, you do not need to know who they plan to merge with or who they plan to outsource work to; however, you will need to know what countries are involved if your client will have any stake or ownership in the relationship. If the person performing this master plan activity is an outside consultant, the executives may prefer to only share this information with the in-house director of security or chief security officer. If there is no in-house staff, the consultant will need to discover as much of this information as possible and may need to sign a confidential disclosure agreement (CDA). (I believe a CDA should always be part of the contract with the consultant.)

The security organization's strategies deal with all aspects of the program from policies and procedures to technology and staffing. Their strategies should be documented so that they reflect where they are now and where they are going. You have probably heard this before, but I believe strongly in the saying, "If you don't know where you are going, you won't like where you are when you arrive!" In order to implement new security strategies, CSOs or directors of security should first address the process of change. This is an area where you, the consultant, can provide advice and counsel, but implementation must be performed by someone in-house. It has been my experience over the years that most people are afraid of change. They would prefer that everything just stay as it is. So the question the CSOs should be asking of themselves is this: "Is change a friend or foe?" The answer to this question is really quite simple: "It's up to them!" Change is a topic that is discussed continuously in the business world. But, as the adage says, "Talk is cheap!" As an example of implementing change I would cite the most dramatic project that I have undertaken in my career. If you have not personally been involved in a major change effort, then perhaps my experience can help you to understand the complexities of this effort. As a part of the reengineering effort in IBM, we reorganized the internal security operation in September 1994. We took the security professionals who were managed site by site by nonsecurity personnel and brought them into one single structure, managed by security professionals. However, this did not in and of itself make change happen. What it did do was to provide the opportunity for constructive, consistent, and rapid change.

Over the next two years we reduced costs by approximately 30 percent, we increased customer satisfaction to 94 percent, and we significantly increased our own security employees' morale. In September 1997, I was awarded the Security Director of the Year recognition by *Access Control &*

System Integration magazine. As people passed on their congratulations to me, I explained that I take credit for one thing primarily, and that is creating the environment where "change" is a "friendly" activity. The accomplishments of our organization are directly attributed to our own people embracing the concept of change and making it happen.

So exactly what did we do to create this environment? Basically, we did three things:

- First, we implemented the use of project teams on as many different aspects of our security business as we could think of. These teams had two goals to accomplish: find the best internal or external practice for the specific area they are looking at and — even more important — increase open communications across the organization.
- Second, we implemented a measurement program to find the defects in our processes. To make this successful, I declared this to be a "no fault" measurement program. The primary "failure" in this program would be if you did not find problems. The secondary failure would be if we did not fix the problem.
- Third, we launched a massive campaign to do national contracts and centralized systems to eliminate as many redundancies and inefficiencies as possible. All of this combined translated into massive change for our people and our strategies in the way we implemented security.

We knew that the only way we could be successful was for our people to see this as something that would be good for them, each and every one of them — personally. To make this happen we first had to convince them that change was absolutely necessary to the survival of IBM and our jobs. You might think this would be obvious to all of us considering our company's financial performance over the early 1990s, but some people have a way of convincing themselves that they are not part of the problem. Therefore, what we had to do was to convince them that change had to happen and we had two choices:

- Deny the need, resist the change, and FAIL, or
- Embrace the need to change and DRIVE that change!

If we, the security professionals, truly and fully accepted this, we had the power to decide our future! If we did not drive change in our organization, someone else would and we would have much less control over the outcome.

FIGURE 1.2 For larger organizations, forming project teams to divide labor and tackle key internal issues is a good way to get employee and management buy-in and come up with practical and creative solutions.

One of the primary tools that we provided to our project teams to do their analysis was the implementation of an internal benchmarking program followed up with a detailed resource and task analysis program (see Figure 1.2). After implementing many of the changes and realizing the benefits of those changes, we then launched an external benchmarking effort. This data demonstrated that we were significantly more cost competitive than any of the other companies we compared with.

As any good business manager can tell you, the best resources of any company are its employees. I personally believe that this group of security professionals is the Best of the Best, but I acknowledge that I might be slightly biased on this point; however, the proof is in the results! It is important to remember that change is not something that you do and it is done. Instead, it is an ongoing process that must be continually driven from senior management down through the organization and by the employees up through the company. This is why it is essential that you create the right environment for change to flourish. A critical part of that environment is your own attitude! Your employees will know very quickly if you are just giving "lip service" to this process or if you are serious. Just as the scenery changes as you travel down a road, your business and even you and your employees must be in a continuum of change. If you are, you will not just succeed, but you will have ongoing success! It is this environment that makes it very important that you have documented, long-term strategies and that you reevaluate those strategies on a regular basis. After all, that is the map you will be using for your trip.

So, what are your clients' strategies? As I said earlier, they should cover all aspects of their programs. It would be very difficult for me to suggest any generic strategies because there are many variations depending on the business they are in. As you develop them, you should utilize the functional team, "the stakeholders" that I spoke about earlier, to assist. Here are some examples of the areas that should be addressed:

- Policies
  - Education and awareness programs.
  - Badge wearing.
  - Clean desk policy.
  - Visitor and contractor controls.
  - Employee involvement and responsibilities.
  - When and how to have armed off-duty police officers onsite.
- Investigations
  - Use of hidden cameras along with determining who should be involved in the decision to use them.
  - Use of a polygraph for interrogations.
  - Whether or not to prosecute employees or others when a crime has been committed (even a minor crime).
- Technology
  - What technologies might be utilized in the future and when, where, and why?

    - What is the migration plan for moving to the new technologies?
    - What is the anticipated end of life of the current technologies in use?
    - Develop a replacement schedule for existing equipment.
- Staffing
    - The use of armed or unarmed security officers documented with the reasoning for the decision.
    - Which positions can or cannot be contracted, regardless of whether they currently are or are not contracted.
    - What style of uniforms should be worn and why?

As you go through the process of helping them in documenting their strategies they will find that they are already following several strategic lines; they just may not have documented all of them before. A good example of this is the use of unarmed security officers. I personally do not like to have armed security people onsite except in rare applications such as a nuclear plant or a top secret installation. Obviously, many CSOs or directors of security feel the same way because the majority of businesses in the United States use unarmed officers. However:

- How many of these security managers or businesses have documented that decision to demonstrate it was a well-conceived strategic decision?
- Was executive management involved in or at least apprised of the reasoning for this decision?
- If a workplace violence shooting were to occur onsite, would they be prepared to defend their decision of unarmed officers in court?

Having these strategies well documented can be invaluable in situations of litigation or even when a decision about an unusual situation has to be made in a timely manner. Their documented strategies should always be their guide.

TECHNOLOGY MIGRATION STRATEGY

I would also like to discuss the issue of "migration strategies" for their changes in technology. If you or they believe they might be moving to a different technology for access control, for example, it is very important that they have investigated the issues around migrating from the current technology to the new one. If the client has a single site or even just two or

three sites, the migration can be relatively easy to accomplish; nevertheless, it still requires a detailed plan, which includes having test locations and education for the end users. By the way, I have seen situations where the end users were not properly educated in the use of the new technology and this set back the conversion by several months; the security team spent countless hours struggling to convince the end users that the new technology was the right solution for the business.

However, if the client has a large number of sites, there needs to be a plan that addresses how they will operate during the migration to the new technology. For instance, when we looked at migrating IBM from magnetic stripe access control cards to proximity cards, there was no existing solution that allowed us to have both technologies in use at the same time without actually mounting both types of card readers side by side so employees could gain access regardless of which card they were carrying.

The solution offered by our vendor was to just take out the old technology and put in the new one. That might be a workable solution for someone who has only a few locations, but for a company that has hundreds of locations and employees who need to be able to access multiple sites, that is not an acceptable remedy. To resolve the problem we developed our own approach. We went to several vendors and asked them to develop dual-technology cards and card readers. Of course, they wanted us to fund the development work for these new products, but we convinced them that this was an investment they needed to make not just for us but to assist any large company that needed a solid migration path to the newer proximity technology. Eventually they agreed and the new products began to hit the market.

Although this provided the hardware solution to our dilemma, that was only part of the final solution. Issues such as importing or exporting databases and conversions of data, education of users, determining who needed dual technology cards and who did not, along with numerous other minor issues all had to be researched and resolved prior to the start of the migration. When you are changing technologies for hundreds of thousands of end users and hundreds of locations, you also have to have a detailed timing plan as well. You cannot make that kind of a change in a few weeks.

My message to you and your client is this:

- Do not assume that the vendors have the right plan for migration.
- Do not let yourself be limited by what currently exists, especially if it does not solve your problem.

- Spend some time investigating others who have made the changes that you are considering and learn from their experiences.
- Make sure you budget some additional funds to help educate the end users on how to use the new technology.
- If the current vendor they are using has never migrated a client of their size to the technology they are considering, they should investigate other vendors to find one that has.

One other approach to be considered is to slowly introduce the new technology into their business. If they currently have proximity access control and they want to move to biotechnology, I would recommend introducing biotech into their high-security areas first. They might want to try the different biotech readers to see which they like best, so they might use the palm print reader in one area, the fingerprint or iris scan reader in another, and so on. This will give them the opportunity to gain experience with the new technology and get feedback from the users and management. If and when they decide to implement it on a larger scale, it is no longer something that is brand new to the end users, as they will all have heard about its use and the migration can proceed in a much smoother progression. Additionally, end users typically feel much better about new technologies if they have been able to provide input into the decision.

EQUIPMENT REPLACEMENT SCHEDULES

I will also review the subject of developing a replacement schedule for existing equipment. The best way to run a security operation is to develop a list of every piece of equipment that the security department owns. This list should be detailed to include the following information:

- Name
- Model number
- Serial number
- Date purchased
- Supplier
- Purchase price
- Location installed
- Supplemental information (for example, if it is a camera you should also include the lens specifications here. If it is a radio, how many channels are on it, etc.?)

- Manufacturer's recommended life cycle
- Projected replacement date

With this information you can establish a replacement schedule for the equipment similar to what the facilities engineering department does for the equipment that supports the building. Once you have this piece of documentation, it can be used during the budget cycle to project future expenditures for keeping the equipment and systems in peak operating condition. Another use of this data is with the contract vendor that is maintaining the systems. Instead of the client budgeting for replacing the equipment, they could have the vendor build the replacement schedule into their annual contract for maintaining the systems. Some businesses find that to be a more acceptable approach to this issue.

One other consideration relative to the equipment that is installed is the documentation of the location and wiring specifications. The wiring specifications should include both the communication cables and the power system. Most facilities these days have their drawings on CAD/CAM or other computer software files. These are files that can be accessed by computer that show every aspect of the facility. However, I frequently find that the security systems have not been included in these drawings; they typically only include the base building information that is used by the facilities organization. This leads to numerous problems whenever these systems need to be upgraded or replaced. It also creates havoc with the systems when there are renovations performed at the facility because the contractor performing the renovations would not have knowledge of the security systems. As the consultant for the client you should review a sample of their drawings and determine if they are fully documented. If they are not, that should be part of your recommendations, and getting them documented should be a part of the Security Master Plan action items.