

SELLING SECURITY

Justifying security projects takes both detective work and teamwork

BY JOHN W. ACOSTA III

In today's economy, many organizations are looking for ways to save money. In light of the current economic situation, company executives have the unenviable task of deciding which programs to downsize and which projects to delay or eliminate. Security programs are not immune to these cost-cutting decisions and in many instances are among the first programs considered for cost-saving.

There are myriad reasons why security programs are so often targets of cost-cutting efforts. In the past seven years, billions of dollars have been spent in the United States on increased security programs, from federal, state and local governments to large and small businesses. This investment has included installation of security technology, changes in policies and procedures, and training. Although there is always a potential for a major security event to occur, most Americans feel safer now than a few years ago. The mindset is no different in corporations.

As a result, the sense of urgency to improve security has also begun to diminish. But the challenge that most facility executives and security directors have is not guarding against some catastrophic event; rather, it is the day-to-day challenge of providing a safe environment

for employees and keeping property and company information secure. The focus of concern is usually not a terrorist plot; instead, it is the events in their communities and the specific security challenges of their working environments or businesses. It is often the difficult task of the facility executive or security director to articulate this point to decision-makers when trying to justify security budgets, especially those that include upgrades and improvements. The task is made more difficult because security is like insurance: No one likes to pay for it, but everyone is glad they have it when something does occur.

Getting Started

Several things can be done to justify budgets and articulate the need to continue upgrades and improvements. The first step is to determine the type

and depth of security required. Look at industry standards and best practices. Threats specific to a given industry should be considered. Most industries have trade publications, associations and networks that address these issues; there are also national or international security organizations — like ASIS International and Homeland Security Industries Association, to name two — that publish articles and provide security information for specific industries.

The next step is to thoroughly understand the threats in a specific physical environment. Most communities generally have the same type criminal activity; the difference is usually only in degree. A business might appear to be in a safe neighborhood, but what is the crime rate in adjacent neighborhoods? In the rest of the city?

Security assessments were recently conducted for two properties, one a high-rise residential building, the other a hospital. Research confirmed that both properties were in relatively safe neighborhoods with low crime rates. However, when the research was expanded beyond a one- to two-mile radius, crime rates got appreciably higher. What's more, higher crime rates were also migrating toward the areas being

assessed. And the crime rates in the neighborhoods where the buildings were located were steadily increasing, with crime trend data from local and national sources forecasting a continued increase over the next five years. This type information is crucial when determining a security strategy and when trying to justify security measures.

Once the threat has been determined,

the next step a security assessment of the current security posture of the organization. Two questions should be asked:

1. Do current security technology, processes and procedures address the current verifiable potential threats?
2. Do the security strategy and budget accurately reflect security needs now and over the next three to five years?

Facility executives often give different

responses to those questions than do security directors. Facility executives normally answer them based on a prioritization of security initiatives against other areas they are responsible for. Relatively speaking, a security program might be well ahead of other programs the facility executive is responsible for, so it might appear to need little improvement.

The security director has a somewhat more narrow focus, and thus might be more tuned into — or overly sensitive to — security needs and feel that the security program is woefully lacking.

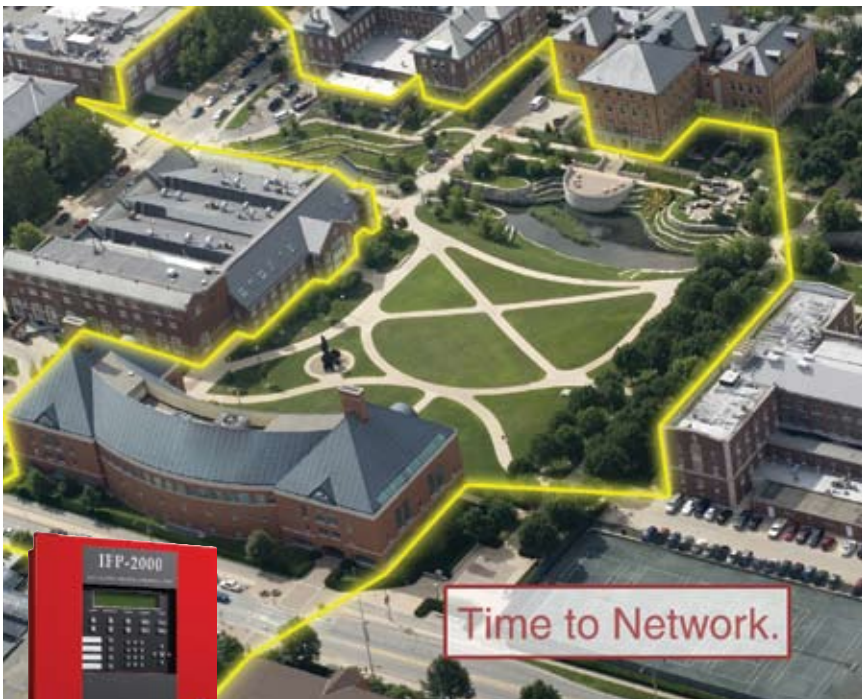
There are virtues and problems with both perspectives. The key to a sound security strategy — and to being able to justify and “sell” security needs to top management — is to strike a balance.

Just the Facts

After determining the threats and doing a security assessment of present security posture, the next step is to determine what the risk is to the organization. Entire books have been written about risk assessment but here’s a brief definition: Determining risk takes into account impact to business activities, likelihood of occurrence and costs associated with addressing the risks.

An example: A threat assessment determines that cars are sometimes burglarized in the neighborhood. The security assessment has determined that there is no access control or electronic surveillance in the organization’s parking lots and that lighting is poor at night.

What is the risk? The business is primarily open to the general public Monday through Friday from 9 a.m. to 5 p.m., and a few employees occasionally use the parking lot after business hours. The risk in this situation might be assessed as low and improved lighting — which could be as simple as replacing burned out bulbs or changing light fixtures — might be sufficient. However, if there were medium to high occurrences of car burglaries and the business operations caused parking lots to be used more heavily at night, then consideration might be given to additional security measures such as improved lighting, electronic surveil-



Farenhyt — Safe...Simple...Smart.

The all-new IFP-2000 is the most advanced fire alarm solution ever offered by the Farenhyt ESD, and the first ever with scalable, network capability. The intelligent, analog addressable IFP-2000 can be networked as multiple panels for one large building or for multiple, independent facilities.

The IFP-2000 is ideal for both new construction and retrofits, and is specifically engineered for growing facilities and campus applications. And like every Farenhyt solution, the IFP-2000 comes with Silent Knight simplicity and dependability, built right in.

So if your application requires a safe, simple and smart fire alarm with interconnection capability, now is the time to network...with Farenhyt.

For more information visit www.farenhyt.com

Farenhyt
Authorized Distributors



**SILENT
KNIGHT**

by Honeywell

Silent Knight • 7550 Meridian Circle, Maple Grove, MN 55369 • 763-493-6400
www.farenhyt.com

More security information and resources are available from ASIS International at WWW.ASISONLINE.ORG and Homeland Security Industries Association at WWW.HSIANET.ORG.



lance and security patrols.

How much risk a business is willing to assume is a senior management decision. It is the responsibility of facility executives and security directors to provide factual information and articulate how their security strategy will reduce risk to an acceptable level. Risk management is important. It can reduce liability costs associated with property damage

and personal injuries — including court costs and insurance premiums — which normally far outweigh the expense of an added security measure.

Bottom Line: Money

Risk reduction is a major justification for new or on-going security upgrades, even in a recession. But other arguments can be used to win funding. Consider

that construction and security equipment costs will continue to rise. As new technology emerges and certain security technologies are more widely manufactured, normally there is a reduction in price. But this reduction in costs will be nowhere near as dramatic as it is for consumer electronics. What's more, labor costs will continue to rise.

It's also important to remember that IT systems in businesses are continually being upgraded. If security systems aren't considered as those changes are being made, compatibility issues could affect the type of security systems that can be installed, thus increasing costs.

Another factor that could increase costs lies in the competitive market. Currently there seems to be an endless supply of security manufacturers, distributors and vendors to choose from. But forecasts show the potential for consolidation, with fewer players in the market, a development that usually brings higher costs.

Beyond pointing out the possibility of higher prices for security upgrades in the future, facility executives and security directors can take several other steps to improve the chances of winning funding for security upgrades.

One important strategy is to form partnerships. It is true that security is everyone's responsibility. In practice, however, security has to compete with all departments for funding. One way to improve the chances of gaining funding is to remember that the goal of security improvements is to provide a safe environment for everyone, including visitors. As the person responsible for security, the facility executive or security director has to find out what are the concerns or needs — perceived or real — of others in the organization. Those concerns and needs can be used to articulate why certain security measures are needed.

That information can be used, not only to form partnerships, but also to find a champion for security improvements. Report those needs and concerns to department heads in an informational way and discuss with them ideas on how those security concerns can be reduced. When formulating a budget, talk with those department heads and let them know that part of the budget request is responding to the concerns of their staff. Another way to achieve this goal is to go to all the department heads and request their inputs when the security budget is being

SMS Security Management System

VICON POWERED BY VICON NET

Harness the Power

Gain the Control

...with fully integrated Vicon SMS Access Control and ViconNet Video Management.

With Vicon SMS Access Control, you can harness the power of ViconNet's enterprise video management capabilities from within your access control interface. Access control events are automatically linked to ViconNet video, creating one of the most powerful, unique and fully integrated systems available.

- Vicon SMS and ViconNet reside on the same IP network, creating a complete security solution
- Standard web browser interface makes it easy to use from anywhere
- Supports access control, event and alarm monitoring, badging,
- VoIP intercom and much more!

Visit us at ISC West, booth #16055

VICON

©2009 Vicon Industries Inc.
All Rights Reserved
Vicon, ViconNet and their logos are registered trademarks of Vicon Industries Inc.

www.vicon-cctv.com
1-800-34-VICON

prepared. Security improvements can be ranked in priority based on the number of requests for a particular item.

Remember the parking lot example? Certain departments may have employees that work at night, and they would be served by having improved lighting in the parking lot. The threat assessment, security survey and risk assessment have indicated the need for improved lighting in the parking lot. Now, that information is validated by employees and department heads who would like to see improved lighting as well. That is a pretty strong justification for improved lighting. Granted, most security justifications do not present themselves that easily, but it is surprising how much people think about security and how often they come up with their own ideas to improve it, even if they don't tell the person responsible for security.

Careful Planning

It is also important to establish a three- to five-year plan and budget accordingly. This is hardly news, but it must be done carefully to be effective.

Suppose the goal is to install a security management system that handles alarms, access control, electronic surveillance and visitor management. In year one, budget for the software program that is capable of operating all the subsystems and a few key peripheral devices. The second year budget can provide funds to add a few more devices, and so on in future years. If in any of the subsequent years the money is not available as planned, the base system is in place and funds can be requested for the next year. A security plan and the budget associated with it are living documents that need to be continually reviewed and updated because needs and events will invariably change.

An experienced facility executive or security director might be fully capable of achieving all these steps, but they can be time consuming, especially when it comes to looking for information or collecting and analyzing it. Hiring a security consultant will cost up front; the return on investment comes in the form of approved recommendations and cost savings. The time it saves the facility

executive or security director will more than likely cover the cost. It can also demonstrate due diligence and lend additional credibility to the security strategy and budget formulation process.

Justifying any budget, especially a security budget, is never an easy task in a weak economy. Many times, funding is driven by emotions. A security plan and budget, however, should be based on facts, available information, experience and input from other departments. Perseverance is the watchword. Continually monitor and update the security plan and budget to be prepared at a moment's notice in the event money becomes available to finance items that may not be initially funded. **EDM**

John W. Acosta III, PMP, CAS, is a senior security consultant for Sako & Associates. A member of ASIS International, Acosta has 28 years of military and civilian security experience. He can be reached at jacosta@rjagroup.com.

E-mail comments or questions to edward.sullivan@tradepress.com.



“B.I.G. CAPTURED THE IMAGE OF OUR COMPANY”
CUSTOM PREFABRICATED BOOTHS
FOR PERFECT FIRST IMPRESSIONS

Visit us at BigBooth.com to find the options that meet your demanding security or site-specific requirements.

Function That Gets Noticed
“We get compliments on the booth from both employees and visitors on how nice it looks. The design is great. The exterior glazing helps reduce glare and the counter top has plenty of equipment room. It has everything we wanted and much more.”
A NASA Laboratory

WWW.BIGBOOTH.COM
South El Monte, CA • Ph. 626-448-1449 • Toll Free 1-800-669-1449