Managing

BY PHILIP S. DEMING, CPP

Proving Security's Value

Demonstrating the value of security in terms of cost savings can make a difference when budget dollars are allocated.

A QUESTION frequently asked of security professionals is: "What is the value of having security for our organization?" Being able to answer that question is key to getting security funding requests approved.

Several years ago, when I was the senior vice president of administration for a large healthcare company, I was asked to attend a meeting at one of our long-term healthcare centers, which was located in a high-crime area. At this meeting, our local security manager offered a presentation, which included a capital budget request of more than $1 million for security. I asked him what return we could expect for investing this amount of capital. His immediate response was that the company could avoid premises liability claims. In response, I countered that property insurance could address much of that concern.

I then asked him what metrics he could offer to show that this investment would yield any marked improvement in the well-being of our employees, patients, and visitors. He was unable to respond.

It was critical for this security manager to understand what was important to business managers and our organizational mission. I met with him later and suggested that he could demonstrate how the dollars he proposed to spend on security would be advantageous to the business managers. As an example, if he could show security could save in labor costs, this would be valuable.

It was difficult for this particular healthcare center to attract and retain the necessary qualified medical personnel because of its location in a high-crime area. The organization had long been aware that turnover among clinical staff, especially, was high. Further, it was more difficult to recruit replacement clinical personnel as compared to other employee positions. If the security manager was able to show that spending money on security would make the environment safer and, therefore, lead to savings on recruiting, training, and retaining healthcare staff across the organization, then this would have a tangible impact on the business.

Several weeks later, the security manager returned with metrics illustrating that for every $1 spent on security, the company could save $3 on labor costs relating to recruiting and retaining employees. That was not counting the more usual savings from reducing equipment loss and other theft. This time, all the business managers were enthralled with the concept of spending money on security as a vehicle to save money on labor costs. Security was awarded its full budget request.

Any security manager can benefit from this approach. The key is to use a systematic approach for developing performance measurements based on presenting valid, reliable, and valuable data; identifying foreseeable risk; and communicating this information to management effectively.

Developing Data

The first issue is to decide which data to collect. In presenting the project to senior management, the security manager in my example began by explaining that, prior to collecting data, his department evaluated which data would be valuable to the organization. Specifically, he collected and correlated data relating to organizational performance—in this case, labor costs and security incidents, such as theft of company equipment and assaults on employees and visitors.

The goal was to reduce turnover by reducing security incidents and making sure that employees were aware of security's success in creating a safer environment. This was particularly important because the company knew that the high turnover was directly related to the security incidents at the facility. Evidence showed that resignations were clustered around violent incidents. And, in exit interviews, employees explicitly stated that they were leaving to find another, less dangerous, workplace. **continued on page 147**

ILLUSTRATION BY RALPH BUTLER

continued from page 148

The department collected data on the cost of reported incidents, which, when divided by the total number of reported incidents, yields an average cost per incident. Security could then track this number over time and correlate it to operational performance. If the trend seemed problematic—if incidents or costs per incident were rising—security could analyze the details to see whether a security response or policy measures would have a tangible impact. The manager provided an overview of the security categories as part of his presentation.

After deciding what to collect, the next challenge is measuring the characteristics accurately. This security manager wanted to measure the cost of security incidents experienced during a given period. Apart from the labor savings and benefits to patient care that would accrue from reduced turnover, among the factors he included to arrive at a cost per incident was the cost of damaged or stolen property. As an example, if computer equipment was stolen, there would be a replacement cost for that equipment. Other variables analyzed included the time the employees were unproductive because they did not have the equipment available to use and any associated costs such as installing software and recovering data.

This security manager focused on developing reliable data. He developed definitions for each type of criminal activity. Having a uniform definition allowed for security personnel to collect consistent and accurate data for the various categories. The accurate data allowed senior managers to feel confident that they could make decisions based upon that data.

Foreseeable Risk

The security manager provided historical references from within the organization and peer references from marketplace competitors to help assess foreseeable risk and evaluate the cost-benefit of security measures. For example, his company had a pharmacy that distributed narcotics such as oxycodone, so he looked at other facilities that had on-site pharmacies and sold narcotics. He used historic and peer reference data to benchmark the level of incidents and to project the likelihood of crimes against the healthcare facility, which ensured that the organization met legal requirements by knowing the risk and taking appropriate measures to counter it.

Communicating the Message

With the metrics and the risk-management modeling in hand, the security manager then turned to the task of communicating an effective message to the healthcare company's management.

Using statistical data can be fraught with problems, particularly if the information can be misinterpreted. Managers should try to keep the data simple to avoid having questions about the numbers become the focus of the discussion.

The security manager also used details from specific examples to drive home his message, keeping the focus on what mattered to senior management. For example, he discussed a recent assault on personnel in the lobby of the nursing home by criminals. He explained how patient care services were disrupted by the incident because the employees involved lost time from work not only from injuries but also because they had to testify in court. He noted that, had the desired security apparatus been present, this risk would have been mitigated. Instead of presenting this example in terms of response times and deployment of officers, the incident was presented in terms of how it negatively affected employees and patient care.

By understanding management's needs, developing good data (including foreseeable risks), and conveying a clear message to management, this security manager was able to win approval of the funds for the capital expenditures for security. ■

Philip S. Deming, CPP, CFE, SPHR (Senior Professional in Human Resources), has 30 years of experience in consulting on security and risk management. He is a member of ASIS International.