

# Extreme Security Program Makeover

*A guide to building or rebuilding your security program*

By Karl Perman and Marleah Blades

Companies are always interested in saving money, but in our economic climate, more of them are trying anything and everything to raise their bottom line. Some are undergoing massive corporate restructuring, some are firing and hiring, and many are asking individual business units to make do with less. These types of situations often call for the re-engineering or from-scratch development of a security program.

Of course, companies that are not struggling also have a periodic need for a fresh approach to security. Some need a formal security program where there has never been one before. Some require security to start over when they shift departmental responsibilities and move it either out of or into the authority of another function. Some just recognize that their current programs are not adequately securing the organization and ask for a new plan, from either the existing security leader or a new one.

If you are that security leader, you have a big job on your hands. If you have been through this before, you are lucky enough to have experience — good or bad — to guide you. But if you have never been asked to develop a program, or if you are simply uncertain how to proceed, it can be difficult to find the kind of guidance you need.

Consider basing your development process on a three-phase plan that has proven itself worthwhile in several corporate redesigns. In most organizations and in most situations, you will



have a good chance of success by breaking your design or redesign into four phases: inventory, interview, assessment and action.

### What Do You Have to Work With?

First, you have to find out what you have to work with. If there is a program already in place, catalog the resources you have available to you. Note that this phase is important even if you have led the security function at this company for years. You may feel you know your assets inside and out, but writing them down in a document or spreadsheet should help you arrange and prioritize assets, remind you of items you have forgotten or underused and point out any redundancies in the use of those assets.

Take a look at the existing systems, policy, personnel, culture, budget and the environment to digest change. What is the main focus of the security department now? What is the reporting structure? What is the budget and where does the money go? Does the function have any advocates within management or among the staff? Who are the primary stakeholders? Is the department outsourcing any of its processes?

You should be able to collect this information from existing documents (such as contracts, budgets, previous risk assessments and communications) and by speaking with the existing staff. If you have multiple sites, go off into the field and take a look around. This first phase can be time-consuming, but it is a crucial foundation for the process. Not only will it give you an idea of how you can redistribute or better use your resources, it will help you to better understand the business' needs and begin to see what is missing at a baseline level.

### What Should Your Mission Be?

Do not jump straight from inventory to assessment. You cannot develop a new plan until you know what that plan is expected to accomplish. If your company is restructuring, your security mission statement may need a little restructuring too.

Set up a series of meetings with the stakeholders you identified in phase one. To develop a successful plan — and to lead a successful security program — you must find out what their desires and expectations are for the business and for

corporate security. If you do not, you may build your new program only to have it shot down by an unconvinced management. You may also find that when corporate executives are not convinced of the necessity of a given risk mitigation measure, their reluctance to embrace it is sometimes translated down to the

employees — who become resentful of the inconvenience the measure may cause. Since the cooperation of the employees is often paramount to the success of a security technology or policy, this could easily weaken your entire system.

When you start interviewing stakeholders, begin by asking them what their goal

## THERE'S A REASON WE NAMED OUR VISITOR MANAGEMENT SYSTEM **EASYLOBBY®**

In 20 seconds or less, you can capture the visitor's information automatically from a license, passport or business card scan, and print a professional looking, full color, customized badge.

**EASY FOR ALL**  
We've been doing this for thousands of customers worldwide for over 10 years. It's so easy to use, we can train anyone in an hour flat, for free.

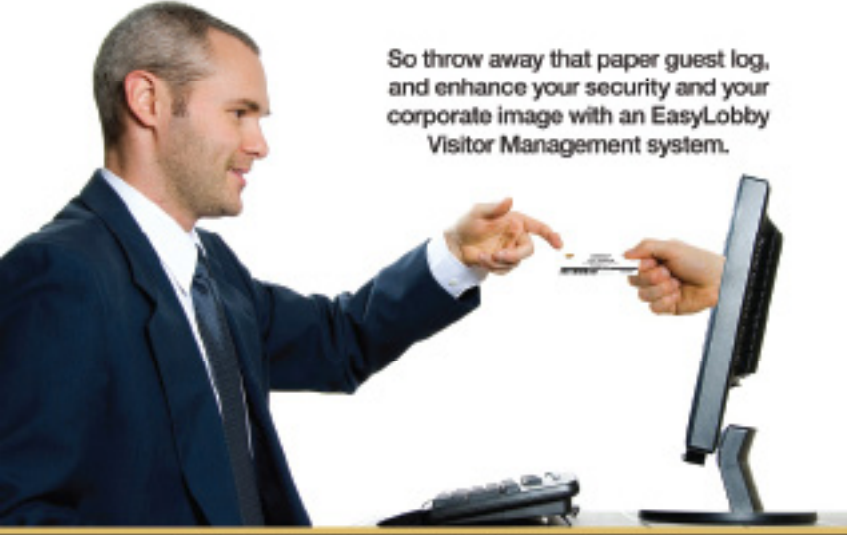



**SCALABLE AND INTEGRATED**  
Deploy one system or a network of hundreds, with central administration. Plus, we're tightly integrated with 30 different access control systems.

**NO RECEPTIONIST? NO PROBLEM.**  
EasyLobby offers a fully customizable self-registration (kiosk) mode for unattended visitor check-in, in 8 different languages.

So throw away that paper guest log, and enhance your security and your corporate image with an EasyLobby Visitor Management system.

**TRY IT FOR YOURSELF AND SEE.**

Contact us today for a **FREE DEMO** at (781) 455-8558, e-mail us at [sales@easylobby.com](mailto:sales@easylobby.com) or visit our Web site at [www.easylobby.com](http://www.easylobby.com)



Visit [www.securityinfowatch.com/stc/einquiry](http://www.securityinfowatch.com/stc/einquiry) and select inquiry #210 for more information



is for their own function or for the business as a whole. Find out the annual business and department objectives, and ask them what they need to be successful. Then start thinking about how your program can assist them in those goals. If HR's goal is to create an environment where workers are comfortable and want to come to work, for example, then check into the state of the workplace violence prevention program, if one exists. See if you have some tools in your toolbox that can help HR reach that goal.

Once you have ascertained the business and departmental missions, then talk to stakeholders specifically about what they want from security. This will almost certainly be a more difficult part of the conversation. Sometimes other executives simply do not know what they want from security — they know they want to be secure, but they may not be able to verbalize the details behind that desire. That's why it is important to come with questions prepared: Where is my jurisdiction? Do you expect me to be involved with investigations, ethics and compliance? Then drill down from there to pinpoint specific action items they want you to accomplish.

Sometimes the expectations of stakeholders are unrealistic. Listen to them, write them down, then think through them after the interview to determine which parts of those expectations can be accomplished and build on those.

## Where Do You Stand?

The next phase, assessment, is about collecting all the information from your inventory and interviews and analyzing it to determine where your existing program is lacking. One of the challenges of the assessment phase is that you have to know what "good" or "effective" security is if you are going to assess the effectiveness of your own program. That is, you will not be able to see what is missing from your program unless you know what the full picture of effective security is supposed to look like.

Experience is the first place you can turn to see potential gaps. Your past observations should assist you in finding some of your program's weak spots. But your own experience may be limited by the industries and organizations you have worked in and the roles you held. In other words, any one person's experiences alone will probably not provide enough insight to help him or her find all the gaps in a new situation.

Industry associations like ASIS International and the International Security Management Association can provide guidance on some of the fundamentals of security. But keep in mind that what might be tried-and-true in other organizations may not work in yours.

The Security Executive Council has worked to develop several tools and resources that set forth a baseline for security programs — a list of the fundamental elements that must be in place for effective security in any industry or type of organization. One of these is the recently released book [Adding Business Value by Managing Security Risks](#), which addresses the core components of a successful program, as identified by Council staff and faculty through many years of research. One of this article's co-authors has successfully used the Council's Comprehensive Security Program presentation for a similar purpose. This PowerPoint also lays out the fundamentals of successful security, enabling users to identify elements that are lacking in their own programs. Resources like these are built on the collective knowledge of many successful current and former security practitioners across industries.

Regardless of the tools and resources you use, your assessment phase should compare your existing program with both the needs of the business and the fundamentals of effective security. Make note of where your program struggles to succeed and where it excels, and use that information to enter the final phase, the action plan.

## Build Your Plan

Create an action plan based on the resources you have, the goals you have identified, and the assessments you have performed. Include action items that will guide your program development from communication to implementation. You likely will not be able to give all your stakeholders everything they want. You will need to prioritize risks, expectations and initiatives to create the most acceptable risk picture.

Again, your peer groups, your experience, and some outside resources can assist you in the writing of your new mission statement and program. [Adding Business Value by Managing Security Risks](#), for instance, includes actual program elements, documentation, examples, templates, outlines, presentations and other components that Security Executive Council community members, faculty and staff have used successfully in their own programs.

Make sure to consider your organization's needs and your corporate culture as you decide how to roll out your new program. In some organizations, you may need to take small steps instead of large strides based on the appetite for change in the organization or based on financial resources. In some situations, you may want to roll out the whole new program in a year, and in others you may want to begin instituting individual policies or implementing new systems one-by-one, to slowly build up to the bigger changes. Some executive teams may want to see immediate, short-term results. Test the temperature of the organization and set realistic goals. If you try to outpace the appetite for change in the business, you risk an early failure that will lose you the confidence of your management and your staff.

## The Work Is Never Finished

Do not neglect to monitor and evaluate what is being done. Make sure what you have implemented is working by instituting performance metrics, conducting regular employee surveys and scheduling regular briefings with stakeholders. ■



*Karl Perman is manager of corporate security programs for a large energy company and a member of the Security Executive Council community.*



*Marleah Blades is senior editor for the Security Executive Council, a risk mitigation research and services organization for senior security and risk executives from corporations and government agencies responsible for corporate and/or IT security programs. In partnership with its research arm, the Security Leadership Research Institute, the Council is dedicated to developing tools that help lower the cost of security programs, making program development more efficient and establishing security as a recognized value center. For more information about the Council, visit [www.securityexecutivecouncil.com/?sourceCode=std](http://www.securityexecutivecouncil.com/?sourceCode=std).*