SEC
SECURITY EXECUTIVE COUNCIL
A research and advisory firm

No Time to Learn

Larry Anderson and Marleah Blades

Originally Published in SecuritySolutions.com
September 2007

No Time to Learn

The transition to a new job is often tough, but walking into the role of security director presents a unique set of challenges that many new hires are unprepared to face. Small issues may pile up quickly and beg for attention, but fundamental cracks within the existing security program must also be discovered and sealed at the outset; the longer they're allowed to remain, the harder they will be to correct.

Consider this scenario: You've just been appointed head of security at a large corporation. At 8 a.m. your first day on the job, you march to your new desk with a sense of purpose and pride. You flip on the lights, settle into your chair and survey your domain. A recent memo catches your eye; it states that all business units are required to submit detailed staff training plans and dates to management by the end of the week. As you pick up the phone to begin following up on this request, a nervous-looking employee appears at your office door.

She's here to find out why there was no security guard to escort her to her car after work last night. She told HR a few days ago that her ex-boyfriend has been sending her threatening e-mails, and they told her she'd have some support from security until she could get an official restraining order. You apologize and say you'll take care of it, then grab the phone again to call the HR director and find out where the disconnect occurred. His immediate response is that it must have been some oversight by your predecessor, who never liked working with HR and would intentionally ignore their comments and requests for help.

You try to smooth out the ruffled feathers, and after hanging up, you flip on news radio. A terror alert in your area has been raised due to unconfirmed threats against local infrastructure. A new regulation is in the works that will determine how your facility controls sensitive information.

The phone rings again. It's the company's general counsel. She apologizes for springing this on you your first morning, but she needs a presentation from you on what the security department is doing to comply with PCI standards. She needs it first thing tomorrow morning.

It's going to be a long day.

No time to lose

Certainly, similar difficulties await a new high-level hire in any field, but while other types of professionals may be able to learn new jobs by doing them, resting easy in the assurance that with time they'll work through the initial uncertainties, security directors have no luxury of time. In the field of corporate security, every unknown, every unresolved problem, may pose a threat to the safety of employees or the security of the organization. Knowing the essentials and having a plan are time-sensitive imperatives.

Unfortunately, while there are plenty of certifications and publications that provide some advice on managing a security program, security lacks overarching industry standards — there's no complete guide, so to speak — so many security directors, whether they're entirely new to the position or just new to the organization, have a hard time figuring out where to start. Any of the following questions could flood the new hire's mind:

- How do I stop putting out fires and create my strategic plan?
- What types of assessments do I need to perform?
- What programs need to be in place?
- Who do I need to know, and how can I gain some influence?
- What kind of strategic and risk management style will be appropriate here?
- How do I get senior management to see my department's value?

If a security director has not experienced these scenarios at other companies or does not have a peer or a mentor to ask, where can he or she turn for help?

Where to turn?

The industry doesn't need broadly applied standards for security management; it's important for all security directors to have the flexibility to make the best decisions specific to their organizations and variables. But security directors would benefit from a set of examples to lead them through the initial phases of a new position and to help them set their priorities. What they need is a single resource that addresses all the critical elements of a complete corporate security program — including physical security, IT, risk management and compliance, among others.

Consultant Ray Bernard contends that a guide of this nature would be extremely valuable to new and transitioning security directors. “The majority of the published work about developing security programs is written from the perspective of ‘starting from scratch’ and relates to the processes, procedures and practices involved. But many organizations have security operations that have evolved over time, are not documented and are all over the map in terms of effectiveness and efficiency,” Bernard says.

“Imagine stepping into a senior security management position in your current company or a new one. You have to learn enough about the business to assess its security risks, from board-level risks down to operational security risks. You have to assess the security people, processes and technology in place in terms of effectiveness and cost and determine how to move forward from there. It would be of great value to have a work that provided guidance for this situation. Since there are no standards for corporate security as a whole, which encompasses much more than just physical and logical security, such a work will fill a concrete need among security professionals,” he says.

Currently no such overarching document exists, but the Security Executive Council (SEC), recognizing the unfulfilled need, is developing a resource under the working title “Security Leadership Essentials” that it hopes will help to fill the void.

A one-stop guide to program management

The Security Executive Council is creating this comprehensive guide based on its body of proven, independent research and resources.

Since its founding, the Council has surveyed hundreds of security leaders — experienced professionals in charge of successful enterprise security programs in both the public and private sectors — to determine the most pressing challenges in security today. These surveys have resulted in a list of strategic initiatives that encompass the top-priority leadership issues facing security directors, including regulation and compliance, cyber-crime, program documentation and risk assessment, crisis management, enhancing influence, strategic planning and business alignment and measuring the value of the security program.

The new Essentials guide will draw from the resources Security Executive Council faculty and staff have already created to help its members tackle these difficult issues, including George Campbell's book, “Measures and Metrics in Corporate Security,” the Council's Regulation and Compliance Management Tool, and the SEC presentation library comprising topics like board-level risk, strategic alignment and Unified Risk Oversight.

The new resource will provide easy-to-reference information on the baselines of successful security management, with a large section of appendices featuring sample forms, contracts and policies. It will include valuable tips in short, easily referenced sections, such as “The Five Most Important Policies to Implement,” “Five Key Metrics to Consider” and “The Five Most Significant Regulations to Know.” Each section will include details on how to develop or correct some of the baseline components of a security program with explanatory graphs and charts. Planned appendices include a model request-for-proposal (RFP), employee referral form and worksheet for calculating the cost of security equipment and installation.

The resource will also include an overview on how to find the data needed to accurately assess the existing security program to help the new hire find areas in need of improvement from the outset.

Again, this resource isn't meant to mandate the form or style of the security program or to provide all the answers. It's intended to help the security director puzzle through some of the most pressing challenges of a new position or program, stimulating his or her thinking with a push in the right direction.

What did you need to know?

The Essentials guide is still a work in progress, and the Security Executive Council is asking the readers of Access Control & Security Systems to provide their input. Log onto www.csoexecutivecouncil.com/sec/five/ to participate in a short survey that will let us know what you think brand-new security directors and newly hired, experienced security directors need to know to get a strong start in a new position. The survey includes questions like the following:

- What are five key presentations a security director should have prepared to show senior management?
- What are the five most important standards or regulations he or she should know?
- What five programs must be in place for effective security?

Look back to your first day in your current job. What do you wish someone had told you? What do you feel you still need to know?

Larry Anderson is editor of Access Control & Security Systems.
Marleah Blades is former senior editor for the Security Executive Council.

Helpful Questions

The new or transitioning security director has to quickly root out the answers to a number of significant questions:

- **How do I stop putting out fires and create my strategic plan?**
- **What types of assessments do I need to perform?**
- **What programs need to be in place?**
- **Who do I need to know, and how can I gain some influence?**
- **What kind of strategic and risk management style will be appropriate here?**
- **How do I get senior management to see my department's value?**

Five Security Programs You Should Have in Place

The Security Executive Council's Essentials guide will provide easily referenced tips for the new or transitioning security director. The following abridged sample shows the guide's current list of the five security programs that must be in place for effective security.

A Baseline Information Protection Program

Information is a critical business asset. The heart of an information protection program is an ongoing process of risk assessment. The resulting information risk management strategy is focused on the preservation of confidentiality, maintenance of data integrity and assurance of the availability of information for authorized users.

A Security Awareness Program

Just as the security policy provides the legal framework for security and sets expectations for those involved, the security awareness program keeps those expectations fresh and in front of those who need to know and understand. Awareness eliminates plausible denial and focuses on accountability.

Safe and Secure Workplace Program

A program for handling workplace violence incidents and threats is essential to protecting the safety and security of employees. This program should designate appropriate reporting structures for threats and define appropriate measures of protection.

Business Conduct Program

Reputation is everything in the marketplace. The business conduct program must have support at the highest levels and must be developed in cooperation with other business units across the organization.

Physical Security Program

Virtually every corporate security program contains some elements of physical security, premises protection and security operations. The physical security program must address electronic security measures and be based on a complete and competent assessment of risk and need.

About the Security Executive Council

We are a research and advisory firm for security leaders. We have a collective of close to 100 security subject matter experts that have been successful security executives or are recognized industry experts in their field. The resources and tools we develop are constantly evolving to provide maximum value. Some engage with us by way of multi-year “retained” services agreements (Tier 1 Stakeholders). Tier 1 Stakeholders are those that want support on an ongoing basis but also want to have an active role in identifying solutions for the industry. Others come to us seeking a specific solution to a contained issue. In all the ways people engage with the SEC the bottom line goal is to help define and communicate the value of the Security organization.

Contact us at: contact@secleader.com
Learn more about the SEC here: https://www.securityexecutivecouncil.com