New Skill For The New Millennium

ALIGNING SECURITY WITH BUSINESS CAN ADD VALUE TO THE COMPANY — BUT CAN ALSO STRETCH RESOURCES

EDITOR'S NOTE: *There are six different areas of knowledge that successful security programs of the future must incorporate, either in the knowledge base of their leaders or in the collective knowledge of the leading staff. They are* ***government elements, security organization, emerging issue awareness, IT security, business elements*** *and* ***executive leadership****. This is one in a series of articles covering each knowledge area. For security professionals, success in the future will be gained only through a blended skill-set — a culmination of all the streams. To read other articles in the series – and to view a self-assessment tool – visit securitysolutions.com/corporate/next-generation-leader.*

BY BOB HAYES, KATHLEEN KOTWICA AND MARLEAH BLADES

Throughout this series we have focused on individual elements of successful security leadership, looking at each skill set in the context of the specific time period in which management homed in on it as a requirement for security professionals. Roughly in each decade since the 1950s, management has focused in on one new skill set as the "silver bullet" for security or the business.

Some hiring managers focused on these new skill sets to the exclusion of other skills that were equally important to the well-rounded security leader's portfolio, while many senior managers instead simply added the new skill sets to their list of qualifications for security leadership.

A few years ago, all the skill sets we have previously discussed—the skills that come from government or military experience, the ability to know and work within the organization, IT security knowledge and executive leadership skills—were considered baseline skills that senior management simply expected to see in security directors and corporate security officers. Then, in 2003 and 2004, another set was added to the group. Management began looking for business skills, such as aligning the department with the overall business goals and adding value to the company, from all its leaders, including those in security. In some organizations, this new responsibility is stretching already strapped security departments to their limits.

History

In 2003 and 2004, extreme competition and Wall Street pressure were taking a toll on corporations and their shareholders. Companies had tried everything to add revenue—cutting costs, increasing quality, improving customer service—but every time one company made an innovative breakthrough in one business area, every other company emulated it, taking away any competitive advantage.

Having exhausted their other options, organizations asked their business units to find ways to add value from within. If a department was considering a new service or technology product, the purchase could only be justified through a statement of how it could add value to the corporation.

Even in areas such as security and IT, which had traditionally been driven by the latest and greatest in technology, new technology had to be scrutinized under the lens of corporate value. Nicholas Carr's book "Does IT Matter?" published in 2004, introduced the idea that IT had become a commodity rather than a competitive advantage, and whichever company could achieve IT goals effectively at the lowest cost would benefit the most.

Security faced a similar shift. Technology such as CCTV and even digital or IP cameras, whose prices were already rapidly dropping, had become commonplace in security programs. Management now wanted more from these investments. Instead of using cameras for surveillance alone, companies wanted to see them shared with marketing departments to determine the effectiveness of sales displays, or with quality control to view the production floor.

Opportunities for security

At the same time, brand reputation and corporate image skyrocketed in value. Company after company succumbed to scandal and an accompanying loss of customers, and they served as an example to all others to protect the brand ferociously.

Security has an advantage here. Many of security's basic responsibilities play a natural role in protecting the brand. For example, student safety and security are extremely valuable to universities, not only for ethical and compliance reasons but also because safety is a reputational issue. Campus shootings like those at Northern Illinois University and Virginia Tech make some parents think twice about enrolling their sons and daughters there. The school that can demonstrate safety and security can gain higher enrollment and community confidence.

Similarly, banks and retailers protect customer privacy online not only because of regulation, but because customer confidence in the security of their personal and financial information is valuable. Privacy breaches result in lost customers, so it's in a bank's or a retailer's best interest to make customers feel safe online.

Security is now a brand advantage in many markets, so adding value is easily within the reach of many security leaders.

The pitfalls of investment and presentation

Two major problems present themselves as security enters into the "value-added" world, however:

- While adding value with security may often seem like a no-brainer, it's far from simple when the security program lacks all the resources it needs to do its job. Management's requirement for all business units to add value makes good business sense, but senior management often does not know anything about what it would take for the security program to accomplish that. They often do not recognize that in order to get value from security, they have to invest in the people and services needed to run security effectively. They also do not always recognize that there are limitations to what security can do. There is only so much security can do when dealing with international laws and cultural differences. For instance, management may not understand why they cannot prosecute hackers from Bulgaria.
- Knowing that you are adding value is not the same as showing senior management how you are doing it. Many security professionals may have a strong sense of the company's goals and how security can contribute to them, but without a program to measure the effectiveness of security, they will not be able to make their case to management.

Where do I get these skills?

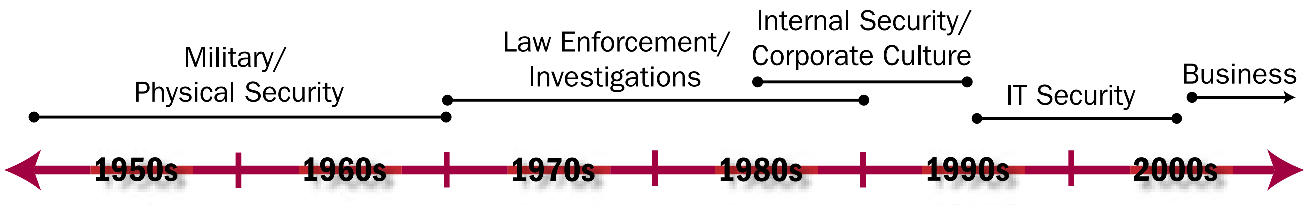
Start by studying the mission and goals of your organization; that is the first step to aligning your department with the business. Get to know the other business units if you do not already, so you can more easily see where your capabilities may match up with their needs.

Develop a metrics program to measure how well various security functions are meeting the needs and goals of the company. George Campbell's workbook "Measures and Metrics in Corporate Security" is an excellent resource for creating a successful metrics program. (Visit SecurityExecutiveCouncil.com)

The Security Executive Council is in the process of identifying the companies and organizations that provide the best training available for each of the six knowledge areas we'll discuss in this series. In the July 2008 issue you will find an entire article on how to acquire the skills needed to become the next-generation security leader.

We would love to hear from you regarding your positive experiences with training programs and courses. Please send your reviews to us at contact@secleader.com. ■

Bob Hayes is the managing director and **Kathleen Kotwica** is vice president, research development of the Security Executive Council, a cross-industry professional organization of security executives devoted to advancing strategic security practices. **Marleah Blades** is senior editor for the Council.



In each decade since the 1950s, management professionals have identified particular skill sets as the "silver bullet" for security and business.

Security Leadership Solutions Executive Council

This article is presented in conjunction with the Security Executive Council (www.SecurityExecutiveCouncil.com), an international professional membership organization for leading senior security executives spanning all industries, both the public and private sectors, and the globe. For more information about the council, visit www.SecurityExecutiveCouncil.com/?sourceCode=access.