How Government Experience Serves Today's Security Leaders

EDITOR'S NOTE: *There are six areas of knowledge that successful security programs of the future must incorporate. 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. To read other articles in the series – and to view a self-assessment tool – visit securitysolutions.com.*

Many security professionals have some form of government background, such as military or law enforcement experience. Chances are, that background has served them well up to this point, but they may well be seeing their career growth stagnating in the face of new requirements for high-level security positions.

Military experience has been a staple of security hiring since the 1950s, when businesses sought to bring the military know-how of servicemen returning from World War II into their security organizations. As private corporations adopted physical security requirements similar to those of government entities, the door opened even further for those with military experience. The Cold War may have also fed business interest in the military background. Emergency preparedness and rapid response took center stage, and these concerns remained important into the 1960s.

Organizations hired candidates with a military background predominantly for 10 to 15 years. Then, in the late 1970s and early 1980s, many began to focus instead on a background in law enforcement. Contracting and outsourcing had gained popularity in many business models at the time; the new employee was no longer necessarily someone known and trusted, but a potential risk. Companies experiencing more internal theft needed more investigations, and they began to hire ex-law enforcement officers who had the knowledge to root out the internal problems.

Strengths and drawbacks to the organization

The influx of military and law enforcement knowledge into security provided several advantages for businesses and the security industry. At the same time, it had some lasting negative impacts.

Advantages

- Those with government backgrounds already know the language of security, including standards and regulations.
- They know the tools of physical security, such as cameras and access systems.
- They are well prepared to deal with certain challenges, such as civil insurrection.
- They maintain a strong focus on external threats.
- Law enforcement knows how to plan and conduct investigations.
- They know how to handle evidence.
- They are comfortable in the judicial process.
- They provide a needed response to growing internal threat.

Possible Pitfalls

- Developing and maintaining the extensive physical security programs often proposed by former government professionals may be very expensive for private business because relying on military knowledge alone often leads to an over-reliance on standards. Securing to standards instead of securing against risks that are specific to a business and location can often lead to unnecessary cost.
- Neither approach stresses the involvement of every employee in corporate security. Unlike fire protection and life safety programs, security programs do not require staff to counsel employees on their roles in security, and management is not assigned responsibility either.
- There is often a culture clash between the corporate environment, processes and behaviors and the culture of law enforcement and military security.

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.

The value of government knowledge today

Clearly, the government skill-set retains great value for security today. Emergency preparedness, rapid response, risk assessment and mitigation all remain fundamental elements of enterprise security. An understanding of physical security elements and processes will also always be a requirement of a well-rounded security program, no matter how the world changes. Physical protection of employees and assets remains a necessity for businesses, safeguarding not only their profits but their reputations. And the need for in-house investigative skills has likely only increased with the advent of the new federal and industrial regulations of the past decade.

Transitioning to the next generation

There are, however, challenges for many security professionals attempting to expand their law enforcement or military skill-sets to meet the needs of today's business-oriented security program. Three challenges stand out for security professionals hoping to transition from this background to a broader context.

- **Regulation and legislation.** New laws and regulations outline detailed physical security requirements that are tailored to certain types of organizations and market sectors, such as banks, hospitals, ports and government facilities. However, it is becoming increasingly difficult to untangle physical regulations from other aspects, for example, information and business requirements.
- **Technology.** The reach and capability of physical security systems and components has blossomed. Data on alarms and system performance is more centralized and accessible; video quality and affordability has increased remarkably; access control can be situated just about anywhere and can incorporate several levels of security. On the law enforcement side, investigations and prosecutions have been significantly complicated by the ubiquity of electronic data; IT expertise is increasingly important in investigations of misconduct and fraud that's based on data that may have been wiped from employee hard drives.
- **Convergence.** The recent rash of high-profile laptop thefts have proven that physical security must be in place for information security to be effective. That said, the increasing inclusion of networked components in physical security systems does require a growing familiarity or comfort with information technology concepts.

The most transferable skills

Luckily, there are a number of major skills that, while not unaffected by the challenges listed above, align with today's business landscape.

- **Emergency preparedness/response.** Businesses and public entities have increased their demand for emergency preparedness and response skills since Sept. 11. These skills include risk and vulnerability assessment and planning, program development, training, information dissemination, development and management of drills and exercises, mass notification and casualty management and evaluation of safety and security needs post-event.
- **Physical security systems.** Events occur every day to remind businesses of the continued importance of physical security knowledge, and their awareness is only heightened with the increasing convergence of physical and information security.
- **Standards and regulations.** The list of laws, regulations and voluntary guidelines affecting security in all sectors is longer than one might think. Dealing with these requires a strong understanding of the security program and the business, authority within the organization, knowledge of all applicable regulations and guidelines, an understanding of the market sector and industry and an understanding of legal and business ramifications.
- **Leadership training.** Maintaining a successful security program means creating leaders at multiple levels of the organization. Leadership training calls for strong communication and interpersonal skills, knowledge of the organization, ability to motivate others, being a strong leader oneself, strong decision-making, management and team-building.
- **Investigations.** Probing the underbelly of the organization to find internal fraudsters and thieves has, arguably, never been more important. Strong investigations require interviewing skills, fact-finding, information-gathering, impartiality, knowledge of the organization and employees, awareness of privacy requirements and understanding of legal limits and allowances.
- **Criminal justice system.** Once investigations are complete, the security professional must know how to assist in effectively prosecuting the wrong-doers.

Where do I get these skills?

There are both traditional and new sources of training and information regarding the development of the skills mentioned above. The Security Executive Council is in the process of identifying the companies and organizations that provide the best training available. A future article in this series will suggest ways to acquire the skills needed to become the next generation security leader.

The Security Executive Council wants to hear about any positive experiences with training programs and courses. Please send your reviews to contact@secleader.com. ■