Security Leadership > Next Generation Security Leader

A Brief History of Corporate Security Leadership and its Future

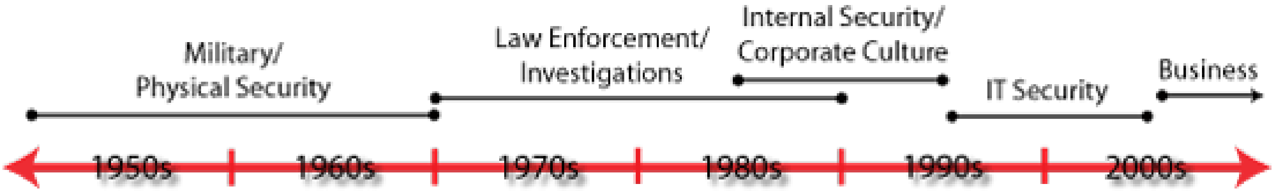
Created by the Security Executive Council

Many security leaders around the world agree that corporate security today requires a range of skills that goes far beyond the capabilities of a traditional security director. In addition to typical law enforcement and military skills, a security leader must understand his or her organization's business from finance and strategy to competition and profits. The security leader must employ executive leadership skills appropriate to the corporation as a whole. He or she must be able to communicate, manage large projects, create strategies, assemble cross- departmental teams, execute plans and more.

A security leader must understand IT security and must maintain an awareness of emerging issues that may affect the company. He or she must follow legislative and regulatory trends, developments in globalization, cyber-crime, security research and development, and other trends that may one day impact the corporation's fortunes.

Today's most accomplished security leaders have both security and business skills, pay attention to emerging issues and must possess an imagination capable of exploring for opportunities that will add value to the company. Today's security world has no defined career path, opening the door for executives with a wide variety of experience; a blended skill set is seen as an advantage. Business will continue to evolve and alter the responsibilities of security leaders.

That is a snapshot of the current state. But it's also important to understand the history that brought corporate security to this point.



Government Experience

Many security professionals have some form of government background, such as military or law enforcement experience. Military experience has been a staple of security hiring since the 1950s, when businesses sought to bring the military knowhow 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.

Corporate Culture Experience

Individuals with government backgrounds held a monopoly on security positions throughout the 1970s. However, in the 1980s it began to change. For 20 years, many organizations had experienced a growing culture clash with their government-trained security leaders, who often adopted a "my way or the highway" attitude in managing their departments and in communicating with other business units and executives.

Corporations began looking for security leaders who knew and understood their company's culture and could work within it-rather than forcing it into submission. They sought out new blood with an understanding of their internal processes, a familiarity with their employees, institutional memory and knowledge of the brand, customers and business. Where better to look than in the organization itself?

Management saw the value of promoting security executives either from within the security department or from elsewhere within the business. Business changes in this time period also reflected an increased focus on internal hiring. Since companies were pushing to get 50 percent of their sales from international markets with a push to globalize the internal force, through the mid-1990s, managers expanded the hiring trend to focus on internal candidates with more international and intelligence experience.

Executive Leadership Experience

In the 1980s and 1990s, companies began encouraging or requiring their employees and managers in all sectors, including security, to bone up on executive leadership skills. Desired skills included the ability to manage large budgets, negotiate, influence peers, coordinate external initiatives, lead staff and communicate and present effectively. Corporations held internal training courses and seminars and incorporated the use of leadership skills more tightly into many of their internal functions. Three main factors contributed to increased interest in these skills among companies:

- International competition
- Quality initiatives
- Technology

In the 1980s, it became clear that foreign competitors were outperforming U.S. companies in several big markets, and business leaders wanted to know why. Their answer was quality. U.S. products and customer service were simply below par. Foreign competitors had espoused widespread use of management philosophies such as statistical process control to ensure that defects rarely reached their customers, while U.S. companies continued to rely on more traditional methods.

In response to this, U.S. corporations launched into a frenzy of quality initiatives. Corporations pushed teachings such as Six Sigma, Total Quality Management and Tom Peters' "In Search of Excellence" to every staffer in every function. Their impact was inescapable. At the same time, organizations were prepping their employees to deal with international business in order to better compete overseas.

Technology also played a role in the focus on executive leadership skills. For one thing, technology was, in part, responsible for the increase in international competition and the growth of the global marketplace. But it also required employees to learn new skills. When e-mail became widespread in the workplace, corporations often held classes on how to communicate appropriately in this new medium and how to avoid abusing this tool in their management activities. As the millennium neared, companies cut down or eliminated their internal training for executive leadership skills due to cost.

Information Security/Technology Experience

Information protection has been around since sensitive information was first put on paper. It resided mainly in government agencies and revolved mostly around internal movement. Files would move about within the organization, but were rarely passed intentionally to external sources. Documents were moved by courier and were stored in filing cabinets, and securing them was a matter of watermarking and carefully controlling access.

With the advent and growing popularity of the Internet in the mid-1990s, information protection changed quickly and dramatically. Businesses were already creating and storing digital data, but suddenly these digital information assets could be moved within or outside the organization within seconds. Information technology security grew to include the protection of files, networks, databases, transactions, applications and more.

The increased use of the Internet led to increased online attacks, which helped to promote the influence of and management support for IT security. A few high-profile attacks occurred, for example, the Code Red worm that infected 250,000 systems in just nine hours in 2001. It raised IT security to even greater prominence. In many organizations; IT security grew into its own entity outside the "security department." This happened in part because many security leaders, who had been promoted through the organization, were caught off guard by the business shift to IT.

Many of these leaders were so focused on gaining the security knowledge that this new vulnerability developed without their notice. Suddenly, it became so large that it demanded attention. By then, the IT organization had created its own security positions-positions that in some businesses eventually outranked the security director to become the leading security offices in the organization.

Business Experience

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 CSOs. Then, in around 2003, yet another set was added to the pile. 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.

The extreme competition and Wall Street pressure at the time were taking their toll on corporations and their shareholders. Companies had tried everything to add revenue-cut costs, increased quality, improved 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 turned to their business units and asked them 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.

Security faced a shift. Technology like 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.

Security leaders needed to start studying the mission and goals of their organization; the first step was to align the security department with the business. They set about getting to know the other business units to assess where their capabilities may match up with business needs. And the start of thinking about developing a security metrics program to measure how well different security functions are meeting the needs and goals of the company emerged.

Now and the Future

That brings us to now. The Security Executive Council sees security leaders that have variations on the experiences and skills listed above. What we're also seeing is a push for top security leaders to have "emerging issue awareness;" and be a strategic thinker, someone able to anticipate, who is adept at planning for current and future needs and is meeting the needs of a changing business environment.

We are also just starting to see security leaders that have a meaningful security metrics programs. Metrics that senior executives care about because they are based on business goals. Security seems to be moving (in some companies) from simply a cost center and a "need to have" to a business-based function that can bring value and articulate that value to the company - at least we are seeing this in the top security leaders we work with. If you are interested in self-assessing yourself on some of these security "value" qualities, then visit this page. After the short assessment you will be presented with a score and some helpful tips on demonstrating value to your organization.

Visit the Security Executive Council website for other resources in the Security Leadership: Next Generation Security Leader

series.

About the Security Executive Council

The SEC is the leading research and advisory firm focused on corporate security risk mitigation solutions. Having worked with hundreds of companies and organizations we have witnessed the proven practices that produce the most positive transformation. Our subject matter experts have deep expertise in all aspects of security risk mitigation strategy; they collaborate with security leaders to transform security programs into more capable and valued centers of excellence. Watch our 3-minute video to learn more**.**

Contact us at: contact@secleader.com
Website here: https://www.securityexecutivecouncil.com/