# Why Companies Turn to IT for Protection in the Information Age

**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.*

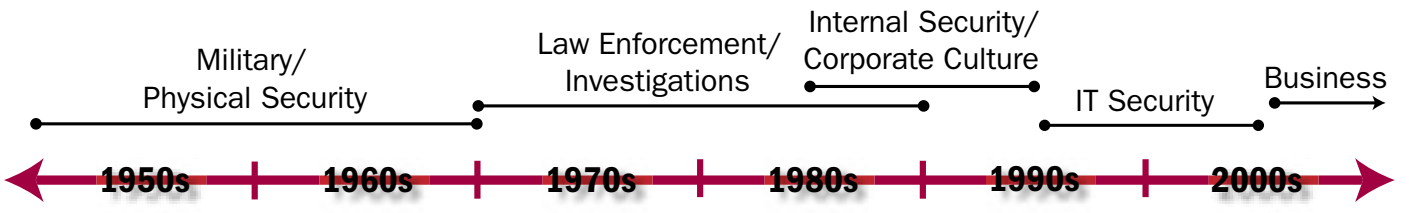
While this series examines the knowledge areas in chronological order, starting with the area that was most prominently hired in the 1950s and ending with today, the big picture of the next-generation security leader is cumulative. Knowledge in all six areas is essential for the security leader who wants to continue to excel at the executive level in the future.

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. That is, 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 much more.

The increased business and consumer 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—such as the Code Red worm that infected 250,000 systems in just nine hours on July 19, 2001—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 the security leaders of the time, who had been promoted through the organization were, in many cases, caught off guard by the business shift to IT. Many of these leaders were so focused on gaining the security knowledge they lacked 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.




**Last month, we talked about the trend that began in the 1980s of promoting security leaders internally up through the organization. This month, we'll begin in the mid-'90s with management's increased interest in hiring from the IT background.**

## Strengths and drawbacks

Those with IT security backgrounds brought valuable knowledge to their organizations:

• **They knew the systems, applications and platforms the business needed to perform at its peak in the information age.** They knew—or knew how to discover—the vulnerabilities of these systems, applications and platforms, and they knew how to shore them up. Basically, they enabled the business to expand safely into the Web.

• **They enabled regulatory compliance.** The information security requirements of the Sarbanes-Oxley Act (SOX) and the Federal Sentencing Guidelines gave IT security a leading role in compliance. Their knowledge of the solutions available and in place helped the business comply more quickly, thus avoiding fines.

• **They created a large body of standards and repeatable processes** that enhanced IT security across organizations.

IT security professionals also brought some limitations to the leading security role. Chief among these:

• **They did not enforce punishment for cyber crime.** Because IT security professionals didn't have any background in law enforcement or investigation, they did not work to stop cyber criminals from exploiting their networks. Instead, they focused their attention on patching up the system once the damage was done. This held true in the vast majority of the IT community, and it led to a preponderance of cyber crime that was almost social in nature because criminals didn't fear prosecution.

• **There was a perception that IT culture didn't mesh with corporate culture.** While many IT security professionals interacted regularly with other departments, other executives often observed their high-tech language and unfamiliar solutions and equated these with arrogance or standoffishness. With that said, certain types of positions often do attract certain types of personality, and the IT personality isn't always team-oriented. In fact, communication wasn't a priority for some IT folks, who created their own space in the organization and often did not venture out to work with other units.

## Transition challenges

This cultural issue continues to be a stumbling block for many IT security leaders who look to move to the "next generation." Although, by the time they have gained executive status, many IT professionals have vastly improved their communication with other departments. However, another communication problem remains. IT professionals often speak in code, discussing security issues in a specific technical language that other executives may have trouble understanding. This can complicate collaboration.

IT security professionals may also struggle to show the business value of their contribution and may have a hard time communicating how some technologies can save the business money.

## Most transferable skills

Of course, the IT professional's technical knowledge and innovation will be key to securing the business of the future. As more business communication goes wireless and handheld, IT security expertise will become even more important. And since online and digital business applications will likely grow in acceptance, innovation in information technology security will serve the business well.

## Where do I get these skills?

There are many avenues through which a security leader can gain knowledge of IT security management. Several organizations offer IT security management certification programs, such as the SANS Institute, the Information Systems Audit and Control Association (ISACA) and the Information Systems Security Association (ISSA). Corporations such as Microsoft, Cisco and Symantec also offer certification. Before joining any of these programs, consider your existing skill level and ensure that the certification is appropriate to that level.

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 a future issue, you will find an article on how to acquire the skills needed to become the next generation security leader.

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