Information Security Career Planning: Education, Training and the Role of Professional Certifications

By Ken Newman

A conversation on information security career planning must be framed around the evolution of the industry. Security evolved from a glass house model in which there were few systems, few applications, few users, and few key requirements beyond accounting for resource usage. Security could be handled as a simple administrative technology task that made sure users and resources did not conflict with one another. The knowledge and expertise required performing IT functions, including security, mapped to only the most basic technical skills.

For many years, security stayed largely static as technology advanced at an accelerated pace. For many businesses, reliance on mainframe hosts gave way to client-server-based networks and applications, and then to external connectivity. Later, Internet connectivity became the norm, and the data that had once been easily protected in one place were spread across the organization, and exposed well beyond. The increased use of technology to manage information produces the greatest risks. Industries have gone through several cycles of disruptive innovation in which security was impacted.

The security function remained chained to its IT heritage in the days of glass-house data centers, and practitioners had neither the skill nor the authority to effectively protect the emerging corporate landscape. Security was primarily buried within the technology organizations of most companies with limited visibility to or understanding of business practices. Security was seen as a necessary evil and an expense, so access to budget and resources was usually limited. During the evolution of the security function, in the 1980s and 1990s, security was a part-time role filled by IT practitioners who understood network technology.

Only in recent years has the security function garnered more visibility and been seen as anything more than an enforcer peddling fear, uncertainty and doubt. Significant regulatory changes around data protection and privacy standards have raised security concerns to the board levels of most public companies, but the availability of properly skilled resources is sorely lacking. It is important that security practitioners have a strong understanding of regulations and that they be prepared to link security efforts to compliance. There has been a long-standing gap of "softer" skills in the information security profession.

Even today, most information security professionals have come from a purely IT background. It has been only in the last decade that certification, training or an academic concentration in security has become more common. However, initial offerings have been highly technical—focusing on system and network controls such as encryption and firewalls.

They have been "teaching information security" and have not broadly evolved to "teaching information security management." Often, the education has not kept up with the regulatory demands of the corporate world. Newly minted security practitioners can implement tools to improve controls, but they cannot procure budget or influence stakeholders to make such tools available.

Career Planning Options

Effective career planning depends upon the right types of educational foundations. Businesses require more and more agility in order to make competitive decisions. More frequently, those decisions involve the management of confidential or sensitive data that may be impacted by regulatory requirements. Poor decisions could produce regulatory fines and sanctions or a breach of information that could erode customer and shareholder confidence. To be successful, the security officers charged with data protection and regulatory compliance need the skills and expertise to

respond quickly to these needs and guide the organization to a path that produces an acceptable level of risk. Creating that kind of capability in the next generation of security professionals requires a broad-based training approach.

There are different types of security training available today. Each fulfills certain needs, and companies may use them alone or in combination for different reasons. The most basic type is general industry training. These courses (often tied to conferences) may be anywhere from a few hours to several days in length. They are often technology-independent or may discuss one or more technologies at a very high level. They provide a general introduction to security and are generally geared toward what kinds of solutions should typically be implemented to meet basic security needs. Companies will often send brand new security people or IT people given operational security responsibilities to these types of classes. They may offer a basic introduction to risk or regulatory requirements, but they do not provide the skills to effectively implement or update a security program.

Similar in terms of time and cost, product-specific training is also available. These courses generally focus on a technology or platform, and go into a greater level of detail on a narrower scope. They can teach someone how to do something such as configure a firewall or use security settings on a server operating system. Companies may use this training for IT staff to improve security as a reaction to some issue such as failing an audit or having a system break-in. They may not have a dedicated security team or a comprehensive security program. However, they have an immediate need to improve security, so they identify a basic element to provide corrective action. They implement the solution and provide training to staff to operate it. As with general training, product training does not provide the breadth of skill required for a successful security professional.

Certifications can be general industry, such as Certified Information Systems Auditor (CISA), or product-specific, such as Microsoft Certified Systems Engineer (MCSE). They require a greater educational or time commitment than the types of training discussed already, because they may involve coursework, practical experience and examinations. They provide correspondingly broader and deeper skill sets that may include the application of basic knowledge toward problem solving. Individuals often pursue certifications to enhance job prospects because many employers use them as benchmarks for hiring. Those companies that have a commitment to development may also support IT or security staff in achieving certifications because they enhance an employee's value to the organization. At their highest levels, these certifications can help someone with broad practical experience support an existing security program, but they still may not provide the ability to step into a role and create or update a program. Further, many without the background or experience can still study (or train boot-camp style) and pass these tests, so certifications alone, while an indicator, are not an absolute benchmark of capability.

Finally, academic education requires by far the most time and financial commitment, but offers the greatest breadth and depth of skills. Individuals may pursue academic degrees when they are confident in their long-term career goals or when they seek to enhance the level of the profession through research and development. Some employers may support this level of personal development, when they understand the clear value that a steady infusion of new ideas, rigorously tested in an academic environment, can bring to an organization. Successful graduates with some practical experience are more likely to be able to implement and influence security programs and, in turn, provide value to their organizations.

To keep matters simple, this article will discuss successful career planning for an information security professional using as its example private-sector corporations with some kind of regulatory requirement for information protection and privacy. Such businesses are revenue-driven and share several common characteristics. They are required to understand and manage risks in their decision-making processes. They also need to be fully versed in the regulations they are bound by to correctly comply with both the letter and the spirit of the law. Such organizations are also marked by a need to effectively communicate internally and externally with various stakeholders to manage their public reputations. Finally, they usually also enforce a strict culture of cost containment to maximize their profit generation. This basic organizational profile will be used to establish what kinds of elements are most beneficial for successful career planning.