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.
KEY ELEMENTS FOR SUCCESSFUL CAREER PLANNING

Regardless of options, there are some key elements that should be present in any form of education in order to provide lasting value to the information security professional. This article does not discuss technical details, although they are acknowledged as core to almost all levels of security professionals. Instead, the article focuses on those areas that create a “breadth” of softer skills in order to produce a more well-rounded and marketable individual.

Understanding Risks
Risk must be every information security practitioner’s benchmark. It is one of the five components required for internal controls under the Committee of Sponsoring Organizations of the Treadway Commission (COSO) Internal Control—Integrated Framework. Risk analysis is a key requirement—not just an ability but as a primary task such as creating policies.

The days when security managers could see the world in black or white, yes or no, are long past. Security for the sake of security is never viable in the corporate world. There must be a risk-based reason behind every decision. This can be especially challenging in larger organizations in which different business areas have different risk appetites.

The starting point should be in the company’s policy and procedure framework. This is where the security professional documents a baseline—if one is not already specified there. Then, they must make sure business owners understand those risks and have measures in place to manage them effectively. Past strategies designed to sell fear or blind compliance are outdated. This is also not an isolated exercise. True risk management is a macroprocess in which the security professional maps risk across the organization.

The value here is straightforward. Expenditures for excessive security can and should be avoided and business operational impact can be minimized.

Interpreting Regulations
Regulatory compliance is the absolute benchmark against which the success of a security program will be measured. The subjects of law and regulation are fast becoming a specialty unto themselves within the field. All publicly traded companies in the US are governed by one or more regulations. In some cases, there may be multiple regulations in multiple jurisdictions. More and more, these regulations include provisions for security that must be balanced against the risk appetites discussed previously. However, regulations seldom spell out exactly how to do something. They just imply what kind of goal is to be achieved.

General regulations have to be mapped to increasingly more detailed governance frameworks, control objectives, and, finally, individual controls. There is power here. Management may not always care about technical security, but they always care about regulatory compliance. The requirements provide an opportunity to get management’s attention and focus it where the risks are. Understanding is also important because different areas of an enterprise (e.g., legal, compliance, risk management) may have different views that the security practitioner needs to be able to integrate.

Communicating Needs
Communication is another one of the five components required for internal controls under the COSO framework. An information security role in an organization may exist only on paper as a box in an organizational chart. The position may actually have no practical power or authority. As such, one of the most important tools to be taught is how to communicate in a meaningful way with nontechnical personnel, i.e., managers.

The practitioner will understand risk and the importance of security, but the manager may or may not even care. The real job of information security is to overcome negative impressions and make sure the manager understands the risk, accepts it, sees its potential impact to the bottom line, and documents appropriate steps to accept or mitigate it. Otherwise, security efforts run the risk of being marginalized.

Security managers rely heavily on training to help business areas handle risk, and making training effective requires strong communications skills. While opinions may differ, the security officer’s goal is to find common ground. In some cases, that may mean knowing when to work with other areas that may have more influence like an audit function. Security professionals must focus on negotiation and collaboration to work within the framework of the organization to ensure that risks are properly addressed.

Managing Costs
Often security groups have very little budgetary authority or financial control. Security products are not brought into an organization because they are new or interesting. Security initiatives must be “sold” just like any other business proposal.
There has to be a specific benefit, reason or return for the investment. In most cases, the security officer has a long list of initiatives and insufficient budget, resources and time. Real-world projects have very different consequences. A project can be successful, but still fail visibly if cheaper alternatives are identified.

They must learn to “know their limitations” within the confines of the organization and prioritize accordingly. Risks will guide where the money goes, and security professionals should be prepared to support other initiatives over their own if they can demonstrate an improvement in security.

Likewise, control or audit requirements should be reviewed carefully. A control is of little value if it is more expensive than the asset it protects, or if it produces too much operational overhead in mitigating the risk. Over time, the goal is to begin to establish a track record by showing improvements with minimal incremental spending. Measurement and metrics are key tools here that can help justify when an expenditure makes sense.

Understanding Business Operations
An information security manager must make sure that the organization views security as a business function and the manager as a business partner. An organization’s security program is made up of four basic components: people, processes, products and policies. They all interact together to ensure the program is meeting its goal of providing adequate controls to reduce risk for the company.

For each of those areas to be effective, the information security professional needs to understand how the posture of any them has an overall impact on the organization. To do that, it is necessary to understand how the business operates. This is a fundamental requirement of risk-managed security. Health care companies and retail stores require different levels of controls to appropriately secure their operations. “Common practices” such as frequent password resets abound, but they may not make operational sense in every business area. However, they often appear in audit checklists, and information security professionals have to be ready to explain variations in light of risk.

A security program must take into account the values and priorities of the business to be effective, and a security manager needs the same organizational knowledge as a business manager to add value. From a career standpoint, this, in turn, adds value to the security manager.

SUMMARY
Risk management, regulatory knowledge, communication skills, cost awareness and business sense are all different aspects of the need for and ability to provide security controls. Thus, the true benefit to the organization is risk-weighted, cost-effective, compliant, operationally viable controls.

The lack of skill or knowledge in any one area impacts the others and, ultimately, the level of control that a security professional can achieve in their organization. Given the importance of a properly skilled and well-educated security workforce and the variety of educational options, the practitioner should assess education, training and certification choices carefully to choose the best course of action to meet their career goals.

EDITOR’S NOTE
ISACA is developing the Career Guide for Information Security and Assurance Professionals, which will be available to the public as a complimentary PDF download on the ISACA web site. Please look for its availability by midyear. Once available, please look for it at www.isaca.org/deliverables. To learn more about ISACA research projects in development, please visit www.isaca.org/research.