Information Security Career Planning: Education, Training and the Role of Professional Certifications (Part 2)

Written by Ken Newman

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 Past strategies designed to sell fear or blind compliance are outdated.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 macro process 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.