

The Next Generation of CISOs

By Patricia A. Myers

Information security has long been recognized as a profession driven by common standards and supported by educational programs and certifications, such as the CISSP, that serve professionals throughout their careers.

History of the CISO

Twenty years ago when I joined the ISSA, the information security profession was in many respects still quite new and immature. Only a fraction of companies, mostly engaged in banking or other financial services, as well as a few government agencies, were establishing information security programs to address regulatory requirements and new threats to their computing infrastructures. These organizations sought to hire experienced and qualified individuals to staff the newly formed functions. Unfortunately, few security professionals could be found with the breadth of experience needed to manage such a diverse function. At that time, colleges and universities hadn't started to offer much in the way of information security curricula, much less an academic degree. Neither were there established criteria for employers to measure an information security professional's knowledge or technical capability.

It was less than two decades ago that several professional societies including the ISSA recognized that certification of information security professionals would play a key role in the decisions of companies wishing to hire qualified security personnel. Information security has long since become recognized as a profession driven by common standards and supported by educational programs and certifications, such as the CISSP, that serve professionals throughout their careers.

Some ten to twelve years ago, there were only a handful of security professionals who had entered the C-Suite. Some of these security leaders began using the title of Chief Information Security Officer (CISO) and had achieved the corporate rank of Senior Vice President, or higher. The term stuck. Now, the CISO title is sometimes more loosely interpreted as the most senior individual responsible for a company's information security, regardless of whether they have been given an officer's title, or not.

Today's CISOs

Today's business world, along with governments and consumers, has come to rely upon qualified information security professionals to help protect its information and privacy. Selecting the right security tools, processes and methodologies, as well as the right personnel, to adequately mitigate risks are important dynamics for businesses to ensure the right fit for the company's culture, risk tolerance, and acceptance of controls.

What are some of the qualities needed for today's CISO? Complex IT environments are the norm in most large organizations. Information security professionals must have a broad range of knowledge, from database systems to networks to operating systems, and must know how to apply technical security controls for them. CISOs must understand how these technologies interact, and how to balance the competing needs of security and the performance and availability of networks and systems, as security controls are deployed in the infrastructure.

The 2005 Auburn University study, *Managerial Dimensions in Information Security: A Theoretical Model of Organizational Effectiveness*, sponsored by (ISC)², found that implementing security programs requires extremely high levels of "task interdependence," with respondents reporting that 62 percent of their daily tasks require the exchange of information or cooperation with other departments. This is a key finding in determining the correlation between top management support and an effective information security program.

Because the CISO frequently interacts with business units outside of IT and with the company's senior management, it is essential for the CISO to understand and speak in non-technical jargon. The CISO must use business terms and communicate *business value* when proposing security initiatives. We have all heard this many times before. Still, it is all too easy to slip back into the comfort zone of using technical acronyms when pleading a case to management!

To obtain buy-in for security projects a CISO must possess business acumen, especially if a project means making a culture change or otherwise poses an inconvenience to the workforce. Sometimes there is demonstrable return on investment (ROI) for deploying a security

Because the CISO frequently interacts with business units outside of IT and with the company's senior management, it is essential for the CISO to understand and speak in non-technical jargon. The CISO must use business terms and communicate business value when proposing security initiatives.

solution, while other times you may call for the solution in order to bring the company into compliance with laws and regulations. Support for security initiatives from senior management is a critical successful factor for the CISO. If senior management do not understand the risks or benefits of the proposal, they're not likely to be in favor of allocating the company's resources to it, either.

If you aspire to becoming a CISO, you may find the following tips useful for acquiring the necessary skills. This advice comes from a panel of experts at the RSA conference held this year in San Jose, California.

- **Learn to collaborate** with other departments. Learn to integrate and appreciate other roles. You must have an understanding of how to tie security into the needs of the business, and effectively integrate feedback from non-technical staff and management into security policies and procedures.
- **Take the value-added approach.** Learn how to align responsibilities and accountability to each department's business goals. Look at the big picture – the goals and focus of the organization. Think in terms of an overall business perspective; know the impact you have on the business, and how what you do creates value for the organization. Communicating the value of information security will help in building a spirit of cooperation throughout the organization.
- **Develop your own security council within the organization.** With representatives from each division of the company, develop your own council to help promote mutual understanding, appreciation and teamwork. When more people agree with your cause, you can create movement.
- **Engage executives in conversation.** Engage executives in conversation so they can get to know you and learn to trust you. These conversations need to be quick and succinct but meaningful, using business terms, not “geek speak” or acronyms. Determine how you can add value to their goals, and then make your case of why you should be consulted or included in a meeting.
- **Offer training.** Another way to build trust is to offer training on security threats that affect home offices, and present prevention techniques. Executives will see the difference you can make to their home computers or networks, which builds their trust

in your ability to make recommendations for the business networks.

- **Learn to balance risk.** Many executives perceive the security staff as not being flexible, so they don't want to invite them into their strategy meetings. Learn to be flexible in balancing security risks with business processes that help the organization meet its goals.

Accordingly, preliminary results of a joint (ISC)²/ISF Study on the current generation of CISOs found the following characteristics important for an effective CISO:

- Has sound management/judgment skills
- Is in a “circle of trust” and is willing to accept feedback
- Is able to “institutionalize” a security culture
- Aligns security strategy with business strategy
- Gets fundamentals dealt with first
- Is sensitive to the organization's risk appetite
- Talks business language
- Maintains technology understanding
- Is comfortable with “uncertainty”

The changing environment

The growing awareness of cybersecurity threats has prompted US federal legislation to protect the privacy of personal information, as well as to ensure the integrity of corporate financial reporting. Due to the increasingly regulated business environment, information security is at the center of corporate governance and the CISO position has become, understandably, more focused on risk management.

It has been said that “good management is good security.” This suggests that those organizations that seek to continuously improve corporate governance have established information security as a viable and equal partner in making the day-to-day decisions affecting the risks to their business.

The next-generation CISO

Looking forward, what criteria or credentials might the next generation of CISOs possess? Surely, with the growing number of institutions of higher learning offering academic degrees in information assurance and risk management, the next-generation CISO is likely to be a graduate of one of the Centers of Academic Excellence. The CISO of the future might possess one or many of the following: an advanced degree in Information Security or Assurance; an MBA; a CISSP certification with a concentration in Information Systems Security Management, Engineering or Architecture; or another similar specialty certification. Having the right security education, certification, and experience coupled with business savvy is your ticket to the C-Suite – as a CISO, if that's where you want to go.

About the Author

Patricia A. Myers, CISSP-ISSMP is Chairperson on the Board of Directors of the International Information Systems Security Certification Consortium, (ISC)²®.