Making Today's Information Security Officer: The Secret Sauce

Book (Excerpt) by Joyce Brocaglia

NOVEMBER 15, 2005 (COMPUTERWORLD) - This excerpt is from Chapter 2, "The Information Security Officer: A New Role for a New Threat," from *The Black Book on Corporate Security* (Larstan Publishing Inc., 2005). It was written by Joyce Brocaglia, president and CEO of Alta Associates.

Gaining a leadership role in security is a challenging job in itself. There is no direct career path, no specified reporting structure, and lots of responsibility with unequal amounts of authority. Nonetheless, many information security professionals aspire to be the Information Security Officer of their corporations.

Executive management teams looking to hire a new head of Information Security typically make it clear that they want an executive who can manage technology-related risk in a way that allows their company to meet its organizational goals. They are not looking for a security technologist to solve specific problems.

So, what does it take to be an effective ISO? Let's review the core skills — or, if you will, the essential ingredients of the "secret sauce":

- A track record of leading and delivering information security and risk management solutions globally.
- An understanding of technology (applications, infrastructure, architecture) and the ability to leverage this knowledge to implement effective security solutions.
- Knowledge and awareness of regulatory and legal requirements relevant to the business.
- An understanding of the business their company is in. An ISO needs to understand his or her industry, their company's place in the market, how laws and regulations affect the company, and how they can add value.
- The ability to manage by influence. Security officers are often in situations where they need to influence change. When we talk about people, process and technology, there's a reason why people come first. If ISOs can't positively influence people, all the processes and technologies in the world won't help. Security is about solving complex problems, and the only way that can happen is to bring people together.
- The ability to communicate effectively and articulate business value. ISOs must know their audience and talk in a language that they understand. This means no "geek speak." The right message must be sent to the right person, in primary colors and whole numbers. ISOs can't come off as "propeller heads" speaking in techno-babble; the ability to talk to employees at their level of understanding is essential.
- A positive attitude. An ISO needs to move from a command-and-control mentality into an enabling one. He or she needs to find ways to say yes. This can be difficult, because part of being a good security person is a natural paranoia, which is not entirely a bad thing. In the words of the poet Delmore Schwartz: "Just because you're paranoid, doesn't mean someone's not out to get you." ISOs must always ponder troubling "what if" situations and try to prevent them. However, the discussion should emphasize the power of defense, rather than the negatives or costs of vulnerability.

Departmental managers should value security as a positive force, not a roadblock. Only ISOs can raise awareness in that regard, by helping other managers understand that the attainment of business goals requires a balance of risk. ISOs can help their colleagues perform the delicate art of risk management, a discipline that elevates security from a necessary evil to a constructive endeavor.

ISOs should possess the personal attributes of confidence, personal integrity, passion, tenacity and a sense of humor. In addition to a healthy sense of paranoia, it is also important for the security officer to have high self-esteem but without the arrogance that often accompanies it. This is a common problem for technologists. It's tough to be exceedingly bright and not be arrogant, but humility is a good thing. It is important to remember that one is an expert for only a brief time, and then more learning is required. For security to be effective, the ISO must always tell the truth and never exaggerate about what can and can't be done. The stakes are too high for ISOs to be anything less than straight shooters.

Is an ISO Born or Made?

Both assertions are correct. An ISO can come from many different, non-security disciplines. Indeed, many outstanding ISOs began their careers in technology and went on to learn security. Some of the most effective security programs are managed by people who have held other significant roles in technology, without security as the mainstay of their resumes. Although ISOs typically have a technology background, more and more ISOs are coming from risk areas with strong project management experience.

The size of the corporation and the department dictate the most desired type of person and skills. A CISO of a major financial institution with a $30 million budget and a few hundred staff who spends a majority of his or her time dealing with regulators, senior executives and evangelizing the program plays a very different role than a CISO of a smaller company with limited staff and budget. They both may require the same skills, but to different degrees. As they set their sights on positions with greater scope and responsibility, information security professionals must recognize the value companies place on solid executive management skills.

Joyce Brocaglia is co-author of The Black Book on Corporate Security *(Copyright 2005, Larstan Publishing Inc.).*