



Career Corner

The New Breed of Security Professionals: Part One

By Joyce Brocaglia
joyce@altaassociates.com

2006 marks Alta Associates' 20-year anniversary recruiting in the information security and controls industry. Over the years we've spoken with thousands of people and developed the kinds of relationships that have given us a unique perspective on the ways that corporations have evolved their approach to security and IT risk. Currently, my associates and I have been striving to identify and cultivate the next generation of Technology Risk Management professionals—the "tri-athletes" who have an understanding of the holistic relationship between the technology, the business it supports, and the discipline of risk management. The demand for these "tri-athletes" is increasing as "The Business" and IT collaborate to establish standardized, repeatable ways to better assess, prioritize and reduce technology risks.

One of the companies that has invested heavily in developing a new approach to security is CIGNA. CIGNA is a multi-billion-dollar company that offers health care and related benefits provided through the workplace, as well as various insurance products. I recently had the pleasure of meeting Craig Shumard, CIGNA's Vice President of Information Protection. As Craig and I spoke, I was intrigued by the approach he and his colleagues are taking at CIGNA. In this two-part series, Craig agreed to discuss CIGNA's approach to security, provide some advice to other security professionals on being more successful and marketable, and how security managers can mentor and build effective teams.

JB: *Why are we seeing this trend towards a more operational risk management-based approach to security?*

CS: A lot of what you're starting to see is because of Sarbanes-Oxley and some of the other regulations that are forcing companies to look at enterprise risk. Previously, risk areas were viewed differently based on specific industries or businesses. Now, largely because of the regulations, people are looking at enterprise risk as a whole, which incorporates all of the business processes or impacts to the environment that could potentially have a negative impact on the business. There are many companies who have hit the headlines who might not have gotten into the trouble that they're in if there had been a formalized process in place.

JB: *So how does CIGNA approach enterprise risk?*

CS: We have someone in our corporate audit function who heads up enterprise risk. This person works with people in each of the business areas to define risk and to roll it out and make it real to the senior managers.

A lot of people talk about doing risk assessments or having the business lines assume the risks, but it's never that plain or cut and dry. For example,

in information security, the first thing you'll have to think about is: what is the risk tolerance of your organization?

Where does your CEO want to draw the line when it comes to risk tolerance?

Does he have a high or low tolerance for risk? The other major issue that you have to decide is who can assume risk on behalf of the organization.

So, at CIGNA we developed a Risk Assumption Model that was driven and fully supported by our CEO.

When I first took on this role over five years ago, we were trying to establish a program where none existed. We often heard remarks like, "That's OK, you don't have to do anything here, we're the business and we're going to assume the risk."

Some decisions that sound innocuous or seem very small can ultimately have a significant impact on the entire organization. So the question is, where do you draw the line on who can assume the risk? For example: an operation in the UK decides they want to save \$50/month by not shredding their documents. Then a dumpster diver goes through the trash and steals sensitive information which gets leaked and the story hits the newspapers. Well, the headline won't read that a small business unit of CIGNA in the UK had a problem. It will say that CIGNA had a problem and lost sensitive medical records. Obviously the negative impact to the organization is much much greater than that business manager may have anticipated. So anytime someone thinks they're making an insignificant business decision to save a few dollars, they may actually be creating a situation with much greater cost ramifications for the company.

Another example would be a business unit that the company plans to divest in a year or two. In an effort to save money, the management stops allocating the resources necessary to implement critical patches. Unfortunately, the fact that they're on the network means a failure could potentially impact other business units across the organization. So, even though a business unit may think that they are the only ones assuming the risk, the reality is that their decisions could negatively impact the whole company.

JB: *So how do you and the members of your team deal with it when a business executive says, "Don't worry about it, I'll assume the risk."*

CS: First of all, for the most part, we try to provide the business with alternatives rather than just saying no. If the business executive is not willing to accept any of the alternative recommendations and says, "It's my business and I'm making the decision," we have a documented process to address this and the way it works is that the business manager can always appeal against our view of the risk directly to the CEO. We've only had a few appeals go to the CEO over the past four years.

JB: *Organizational reporting structure seems very important for this to be effective.*


CS: Yes, very much so. I report to the CEO but have made it a priority to develop a strong relationship with senior business leaders across the organization. Reporting relationships, the approaching and attitude of your company's CEO, and your ability to build a rapport and working relationship with your peers in the business units all contributes to the success of your security program. Being able to communicate your initiatives and findings in terms that can be easily understood goes a long way to building success.

JB: *You report to the CIO, but if a business executive wants to appeal your view of a particular risk they must address the issue directly with the CEO. Why is that?*

CS: The CEO's perspective is that he is the best person to have an overall view of the risk and impact that a risk decision will have to the entire corporation. It is possible that the CIO may not pay security the attention that it should. For example, during budget time, given the fact that security is something that traditionally people feel adds complexity and cost, it might not receive the consideration that it should. The CEO is looking at it from the standpoint that "the buck stops here, and I have the best vantage point to see the entire picture."

Conclusion

In summary, Craig Shumard has shared with us his approach to developing and implementing CIGNA's risk assumption model, which integrates security into the culture and everyday activities of his organization.

We will continue our conversation with Craig in next month's issue of *The ISSA Journal*. Craig will share his insights on topics such as: which skill sets are most important to be an effective security leader, how to cultivate the next generation of security professionals, and how to move your department towards a more risk-based mindset regarding security. 

Joyce Brocaglia is the CEO of Alta Associates, the Human Capital Risk Managers specializing in information security recruiting. www.altaassociates.com