



# Career Corner

## The New Breed of Security Professionals: Part Two

**By Joyce Brocaglia**  
*joyce@altassociates.com*

In last month's article from *The ISSA Journal*, we discussed an emerging trend in corporate America. Companies are changing their focus from information security to information risk management. One company that has invested heavily in implementing this new approach is CIGNA. CIGNA is a multi-billion-dollar company that offers health care and related benefits as well as various insurance products to millions of customers. Craig Shumard, CIGNA's Vice President of Information Protection, and I discussed how Craig developed and implemented CIGNA's approach to Information Protection. Last month Craig shared his thoughts on risk. This month we continue our conversation.

**JB:** Does CIGNA still maintain the traditional security roles in its new model?

**CS:** Yes, we continue to have functional security experts in the areas of vulnerability and risk management, engineering and standards, incident response and business continuity, policy awareness, and compliance.

One way that we ingrain security into the business and not make it "someone else's job" is by creating information protection coordinators and information protection champions. The champions work with business managers to integrate security into the company's lines of business. The coordinators have their own job but also work with security in providing insight as to what is relevant and important to their particular business area's needs.

**JB:** Where have you been finding professionals with integrated skill sets?

**CS:** We have found many people internally. Some come from rotating through positions within the company. When going outside of the company for staffing these positions, I would look for people who had a background in IT audit or consultancy along with business exposure.

**JB:** Are you speaking with those on your staff who are in more traditional roles about the importance of gaining business understanding? How are you cultivating these people?

**CS:** I think there's a different level of progression. We have senior staff in our architecture and engineering group who regularly meet with business leaders, who go out on customer calls and who work with lines of business project teams so they can integrate our message into daily operations. Vulnerability and risk mitigation groups deal with the lines of business to a lesser extent, just due to the nature of the type of work that they do.

The compliance and risk team probably interfaces with the business teams even more so than the information technology teams. Probably half of my staff interfaces with the business people more than the IT people because of the way we're structured.

We put a lot of emphasis on the value of bringing professionals in from the business to address our staff and we encourage town hall meetings. For example, we'll have someone from sales and marketing come in and talk about new products initiatives and marketing thrusts.

**JB:** Have you found that some security professionals who want to move into executive roles lack the leadership skills and communication skills necessary to obtain a job like yours?

**CS:** That's a really good point. The biggest areas we've had to work with our staff on is their communication and writing skills. Engineers are very good about framing risk and talking about issues from a geeky standpoint, but if you gave their paper to a business person, they'd have no idea what they're talking about. So we spend a lot of time and resources working with them to be more oriented and focused towards the business. This is something that takes time, but it really pays off. Not only do they start to write differently, they start to think differently and we've found it to be extremely beneficial.

**JB:** So what advice would you give to someone who has a solid technical background but wants to move her career to a more management role?

**CS:** The key skill is your ability to communicate. You have to be able to sit down and have a conversation with senior managers without having their eyes glazed over about the technology. You need to be able to frame your message very simply and elegantly so they understand what you're trying to tell them and you also have to have enough business knowledge to convey your message in a way for them to understand how it will impact their business.


**JB:** What advice would you give to a technical professional who wants to gain business knowledge?

**CS:** There's a number of ways for security professionals to get an understanding of the business their company is in. Two suggestions are: First, look within your own company for a rotation opportunity. Even if it's a side step instead of a forward step, if it allows you to have in-depth exposure to a line of business other than technology, it could be a valuable way to gain business acumen. Second, volunteer to be on specific projects representing your department. For example, some of the professionals on our team who are participating in off-shoring projects are learning about business issues and what we're trying to solve, and working on a team with business people, you start to gain business acumen.

**JB:** If you're a security manager who wants to move his or her department towards a more risk-based approach, what steps should you take?

**CS:** I think it's incredibly important to begin having discussions around risk as opposed to technology. By combining this approach with security bench marking, it will be easier to build allies across the organization and present to management about where you are and where you need to be. This approach makes it easier to highlight potential risks, prioritize them, and make better business-based decisions on how to address them.

## Conclusion

So there you have it, straight from the top. As our profession evolves it's increasingly important that "information security professionals" take a leadership role in changing the ways that people think about their roles. It's not just about protecting information assets and preventing the bad guys from doing wrong because that is only part of the puzzle. The next generation of "information security professionals" will be those who can work with executive management and business stakeholders to more effectively reduce business, organizational and technology risks collaboratively and effectively. By taking this approach, we will all be closer to making security part of *everyone's* job. 

---

*Joyce Brocaglia is the CEO of Alta Associates, the Human Capital Risk Managers specializing in information security recruiting. [www.altaassociates.com](http://www.altaassociates.com)*

