



Trusted Advisors on Risk Management

By
Leigh Henderson
Editor, *Spyglass*



L-R: Joyce Brocaglia; Rhonda MacLean;
LJ Johnson; and Simone Seth.

Today we live in a world being continuously bombarded by new technology, advanced threats to our corporate operations and individual well-being, as well as increased need for better strategies to insure more effective business resiliency and disaster recovery.

I sat down with three members of the Executive Women's Forum for what turned out to be a wonderfully interactive session. The professionals below represent 75 years of Information Risk Management (IRM) expertise and share their perspectives on the field with *Spyglass* readers:

LJ (Lisa) Johnson, Global Information Security Officer, Nike, is responsible for defining and driving the company's worldwide security program including technology architecture, policy management, regional implementation, security awareness and operations. She is also involved in developing comprehensive Intellectual Property Protection initiatives within the organization;

Rhonda MacLean, President & CEO, MacLean Risk Partners LLC, provides practical security and operational risk management consulting for organizations worldwide. Strategies are aligned to meet client-specific business objectives while addressing industry-specific operational risk management requirements; and

Simone Seth, Advisory, PriceWaterhouseCoopers, is leading the North American efforts of the Information Security Forum (ISF), a not for profit association, dedicated to researching and writing about leading information risk management and information security business practices in today's global marketplace and forecasting trends in the arenas of security, privacy, governance and compliance.

Shattered: The field of information risk management is not new. Discussions on the topic have become more widespread – making their way into corporate boardrooms. What are the key factors driving this awareness?

Rhonda:It's a combination of factors. Publications and headlines are highlighting the issues around security, business continuity as well as privacy concerns of individuals. Corporations are looking for ways to promote confidence in their controls and handling of customers' private information. Many executives have put this topic at the forefront of their business agendas.

LJ:Corporations are responding as the consumer becomes more aware of their vulnerability. Three to five years ago there were no articles in general newspapers. Recently, USA Today had an article on it.

Rhonda:Also complying with multi-national privacy laws around the world is making IRM an increasingly important and complex issue for executives. .

LJ:Financial damages have increased significantly and corporations are becoming more aware of the risks.

Simone:Breaches of security are newsworthy. Companies and individuals can easily purchase off-the-shelf technologies. When users are more technology savvy, they become a higher level of risk. For instance, an employee can bring a wireless router into their office and with a little bit of knowledge, interfere with or even bring down the corporation's entire system.

Rhonda:Technology is not the only answer to meeting the challenges in putting together an effective information risk management program. Process and people are both key ingredients. I would have to say that people play the major role in protecting sensitive information. That is why risk officers need to focus on three things: people, process, and technology. With heavy emphasis on people.

LJ:People are the weakest and biggest link.

Shattered:What are the challenges of being leaders in the IRM field? How do you meet these challenges?

Rhonda:What we do is problem-solving. Our work is to be open, listen, and understand. It's a wonderful career.

LJ:I agree. We try to fix things that can't be fixed. It's the game, the stimulation, the ability to try to make things better, that's the challenge. And part of that challenge is changing corporate culture. We cannot make these changes ourselves. People are having to be more accountable.

Simone:Women have led the charge in demystifying the field. Truthfully, I hold myself accountable for not being well-integrated into the business units earlier in my career. We created a mystique. Then we started asking ourselves, "Why aren't we more integrated?"

Rhonda:We have numerous leaders in this field who have the skills required to work with the leadership level of their organizations. Some of the skills include being a team player, a good listener and clear communicator.

LJ:I'm transitioning my own staff to understand the business units first in order to better translate the value proposition we are presenting. This is a very hard transition for people with lots of letters behind their names because we have to focus on actions and interactions. Traditionally, we in technology have wanted to grab the wheel, drive the car, be in control. In our new role, we don't drive but instead we hold the map for the business units, and assist them in getting where they need to go – based on their tolerance for risk, we can help them navigate the potholes and find short cuts, too. We are moving towards being trusted advisors and not just security geeks.

Rhonda:There are regulations on the road they're traveling as well. Technology needs to be aware of and know the global rules of the road. They need to team up with others such as the legal department, regulatory organizations, and internal and external auditors to name a few.

Simone:Everyone has something they need to do to define and create an IRM formula for long-term success. For 20 years, there has been management of all aspects of internal controls for risk – by different individual groups. The client became fatigued by so many people approaching them for assessments on risk factors that the overall picture wasn't being filled in. Clients couldn't digest all the information so we're simplifying and unifying our approach to put it in one bite now.

LJ:Budgets are tight and companies are looking to reduce operations overhead. We are overlapping in areas where we don't need to be.

Simone:The right approach is to make an enterprise-wide global scorecard. My philosophy is, let's be on the same page with the same tools if we're truly going to assume the role of trusted advisor.

Shattered:I heard during this conference that, "We believe everything can be translated into numbers." What's the impact of IRM on a company's bottom line?

Rhonda:The IRM value proposition is so important. We need to be able to measure the costs and the success it brings to each business unit and the company as a whole. This helps greatly in making risk reward decisions.

Simone:You're talking about the metrics of security. We have to present what we are doing in language that people understand – and that language is numbers. As one of our speakers this morning said, you have to know exactly, "What is the problem?" We need to be able to listen and respond appropriately to what we hear. Then translate that information into an ROI statement – what will the client get from their investment in risk management.

Shattered:What's the greatest career challenge you've encountered? In what specific ways did you overcome it?

Simone:My challenge was working for people who didn't understand the subject matter for the longest time. I stumbled along, finding mentors and coaches – like Rhonda and Joyce (Brocaglia, CEO, Alta Associates) who helped guide my career.

Rhonda: My greatest challenge was convincing CEOs/executives they needed a shared responsibility and shared accountability approach for operational risk management. To promote the implementation of a shared accountability approach, written performance objectives – which have metrics to measure effectiveness – were essential. Having written performance objectives placing effective IRM as one of the key measures of an executive's success drives faster cultural adoption of IRM. Executives need to know, "What's in it for me?" and once you can demonstrate what that is, it is much easier to get them on board.

LJ: I remind myself, "What am I going to be held accountable for?" Making a transition from being a technical expert on security to building business skills has been a challenge. I needed to learn how to truly influence and get the customer to understand the business proposition. Going back to school for a master's in business and technology helped me as did finding mentors. I pushed myself out of comfort zone and into new space. For instance, as a 'fire fighter,' I know what to do to satisfaction. Now I'm not as much of a hero – since I work on preventing fires before they start. I've learned how to let go and be more of an advisor.

To Attend this year's Executive Women's Forum on Information Security, Risk Management and Privacy click here: www.infosecuritywomen.com.