SPECIAL INTEREST FEATURE

PREDICTABLE SURPRISES

Understanding the IT risks that are specific to your business will not only help mitigation efforts, but may assist in turning them into opportunities.

Managing risks in your company is a job in itself. In today's world of 24/7 connectivity and online access, risk and security are always top of mind for most companies – especially when it comes to information technology, or IT. Most individuals, whether they are technologically savvy or marginally informed, can easily understand the implications of such breaches. Tony Ritlop, a partner with Ernst & Young's Advisory Service Practice, knows all too well the emerging risks that companies are facing within their IT departments.

He points to four main issues at stake:

- Cloud computing
- Social networking
- Mobile computing
- Big data analytics

Ritlop says many companies have a "silver bullet" mentality when it comes to their technology. "A lot of people think they're going to put their information in the cloud, for example, and not have to think about it. Not at all. You have to manage it – you have to manage your vendors."

Security risks may seem specialized, but they are assessed under a general sphere. For example, The Technical Standards and Safety Authority (TSSA) uses two methods for assessing and analyzing risk.

The first, according to Michelle Reid, TSSA's Team Leader, Enterprise Risk Management, is through "SWOT" analysis (Strengths, Weaknesses, Opportunities and Threats). "Typically, it involves understanding the internal and external strengths the company has," Reid explains. "What are the competitive advantages? Where do they excel? And where are the weaknesses?"

The second method that TSSA employs is the internal Enterprise Risk Management processes itself, which involves management team members assessing the objectives for the organization.

Social media has also become part of the IT culture over the past number of years, and possess its own set of risks. The biggest risk, according to Ritlop, is that employees don't get sensitized to the social media universe, and the downside of going viral.

With social networks, Ritlop notes, companies need to educate. "It all boils down to someone doing something wrong because they just didn't know." Companies can introduce security that either supports softer policies or enforces stricter ones. But it's the culture of the organization that will determine its IT security policies.

Interestingly, even though IT is so specialized, Ritlop says you don't really need specialized tools to analyze or assess the risks. However, companies might need IT experts who understand the technology. "That's all execution," he says.

> *Technology is just one part of risk management. People and processes make up the other parts.*

Another issue especially important for small businesses relates to mobility. "Small businesses, which support mobility amongst their workforce, need to be as policy-based as large organizations," he explains.

The fourth of Ritlop's IT emerging risks relates to data storage. Often, small businesses have that relevant information in multiple places, but if a small business is serious about mining their data, they need to ensure it is stored properly with one source.

Ritlop stresses that technology is just one part of risk management. People and processes make up the other parts. "Any good advisor will give you a roll-out plan," he says. "But," adds Ritlop, "a really good advisor will give you a plan that tells you how you, in your organization, should do it." ■