



Career Corner

A Risk By Any Other Name...

By Jeff Combs

The Security industry had been abuzz with talk about Risk Management. Technology Risk, Compliance Risk, IT Risk, Operational Risk...and the list goes on. I've even written a previous column on the shift in our industry from a technology-driven information protection culture to a business-driven risk management culture. The reason behind this shift is that organizations are facing an increasing range of threats that require better coordination between security, audit, the business, vendors and management. By looking at an organization's vulnerabilities from a broader "risk management" perspective, decision makers can better prioritize threats and deliver the assets needed to address them. Not surprisingly, as this is happening, more companies are rebranding Information Security by calling it "Technology Risk Management." And more Information Security practitioners are referring to themselves as IT Risk Management professionals. This is where the confusion starts.

Information Security vs. IT Risk Management

Confusion, you ask? Yes, because there is a real and significant difference between Information Security and IT Risk Management. As a result of working with large multi-national clients, especially those based in Europe or who have significant holdings in Europe, my associates and I have been tasked with understanding these differences. For the purpose of this column, I'd like to help clarify what IT Risk Management is in relation to Information Security so that readers of *The ISSA Journal* have a better handle on the terminology being used.

IT Risk Management can be defined as the discipline of designing, developing, sustaining and modifying operational processes and systems in consideration of applicable risks to asset availability, integrity and confidentiality. IT Risk Management is about taking an analytical approach to the whole IT operations and support cycle so that process owners can make better, more reliable decisions on how to address risk. As a result, the appropriate protection assets are focused on the areas of greatest priority, leading to better efficiency, cost effectiveness, and operational performance.

That's the high-level description of what IT Risk Management's objectives are. The idea is that when a company takes a consistent approach to addressing **all** IT-related risks, the organization will have a more integrated way of addressing them. So what kind of risks are we talking about if we're not talking about information security risks? There are many, and developing an organization's risk profile really depends on the business they're involved in. That said, here are some examples of what I'm referring to:


- ▼ Compliance Risk—the inability to effectively audit processes and systems against requirements and/or meet compliance requirements.

- ▼ Availability Risk—the inability to process business transactions due to system failure or interruption.
- ▼ Performance Risk—the inability to service customers and meet expectations.
- ▼ Scalability Risk—the inability to effectively handle increased demand for services.
- ▼ Recoverability Risk—the inability to recover lost data critical to transaction processing and reconciliation.
- ▼ Human Capital Risk—the loss of intellectual property due to staff attrition.
- ▼ Outsourcing Risk—the loss resulting from reliance on a third-party vendor that fails to deliver critical services.

These examples demonstrate that there are a range of IT-related risks beyond the vulnerabilities security professionals commonly deal with. But you can also see that the efforts of security professionals have a direct effect on the impact many of these risks can have. If inadequate controls are in place, your company will fail its SOX audit. If a worm crashes the network, core business transactions come to a standstill. If your Web site gets DDOS'd and customers can't access services, you could lose them to a competitor. If critical data is lost or stolen, your company could end up on page C-1 of *The Wall Street Journal*.

However, despite the fact that Information Security is directly involved in mitigating many of these risks, it's inaccurate to refer to "Information Security" as "IT Risk Management." They are not the same thing, and while it may just seem like semantics, it really isn't. In Europe where the field of IT Risk Management is well established, it is clearly distinguished as being different from Information Security. Information Security is *a part* of a company's IT Risk Management strategy, not *the* IT Risk Management strategy.

Conclusion

Given that more and more of the Security resumes I read refer to IT Risk Management in the wrong context, I wanted to shed light on the difference and meaning of these terms so that InfoSec Professionals don't mischaracterize themselves. It may seem like splitting hairs now, but it's now always going to be this way. It's a fact that the way companies manage technology risk is evolving and it's moving towards the broader context of IT Risk Management. This shift isn't going to happen overnight, but it will happen because it gives organizations the perspective and approach needed to make better decisions on how to manage their risk portfolio. 

Jeff Combs has been with Alta Associates since 1999. Jeff has a depth of experience recruiting security professionals at all levels for corporate clients, professional services firms, and security vendors.