The ‘Risk Gap:’ Business Perspectives on Security

By

Bruce Murphy, CISSP
Chief Executive Officer, Vigilinx

The dramatic rise in the pace and sophistication of cyber attacks is resulting in real financial and operational losses to major corporations. In addition, the events of 9/11 have highlighted the vulnerabilities infosec professionals must address to protect our technology and information infrastructures from cyber-terror attack.

At the same time, most organizations cannot afford to allocate the dozens of resources required to properly mitigate this problem. So this is creating a “risk gap” that will continue to grow unless infosec professionals develop new and innovative approaches to managing information security risk. This entails delivering sound business practical solutions to the enterprise.

As we entered the new millennium most agreed that security would become a No. 1 priority among purchasing agents around the world. Instead, a depressed economy dragged IT spending down sharply. Unfortunately, the belief that security spending would be immune to economic downturn proved to be wishful thinking at best, self-delusion at worst. So the spending ramp did not materialize and the security practitioners of the world have had to do more with less.

As security professionals, we deluded ourselves into believing that the floodgates of security spending would be opened up and the budgets of every CSO would double and triple. This, sadly, is not the case. The truth of the matter is that mainstream business people still view IT security spending as overhead and not a core business process.

Even the most jaded CFO will admit that security is important and many senior executives repeat that message on a daily basis. But where the rubber meets the road is when the jaded CFO starts allocating larger budgets to cover information security. And that is just not happening. The reason is simple - security spending does not drive revenue for your average manufacturing company, or any industry for that matter, and is not at the top of the list of core business needs, at least for most businesses.

The infosecurity profession needs to begin to address the root cause of limited investments in security and develop creative alternatives to 1) Develop cost-effective solutions, and 2) Deliver value to the enterprise through information security.

Remember that the CFO has two major criteria driving his investment decision-making process – initiatives that make money and those that save money. Every infosec initiative has to explicitly fulfill one of these two tenets or it will fail before it begins.

The InfoSec Evolutionary Timeline

Understanding how we navigate the security minefields can be realized by understanding how the profession has evolved. The discipline of information security is a fairly nascent profession being arguably in meaningful existence no longer than 40 years or so. In that time we have experienced a few metamorphoses that have been fairly dramatic.

These can be described in five key stages, or phases of development:

The Dark Ages – Information security began in relative obscurity in the mainframe world focusing on access and file permission in a relatively controlled environment. Most networks were closed by today's comparison and the risk level was considerably less than it is for modern IP infrastructures. As a result the effort required to secure information assets was not particularly large and not viewed as particularly important. Many of the individuals who were assigned security responsibility had them assigned to them opportunistically or as a form of last resort.

Enlightenment – When computing power and information migrated outside of the data center walls into distributed client/server environments, security needs grew dramatically. Significantly more attention was paid to security and an understanding of the complexity of this issue started to hit the radar screen of many.

Internet Age – When the Internet Age burst upon us we experienced a dramatic wake-up call for the level of security exposure facing us. Reliance on an infrastructure designed to facilitate redundant paths of communication while "anonymizing" the user base is an inherent security nightmare. As a result, companies spent huge amounts of hours and dollars trying to shore up the infrastructure they were currently using to transact significant elements of their business. During this time, security resources came into high demand and finding the right security answers became more elusive. As a result, security focus became higher and expectations for massively increased expenditures grew quickly.

Age of Reality – In the post-2000 world, recession hit and severely hampered the growth of the industry. The massive ramp-up in outsourced managed services and enhanced expenditures on all forms of security products, people and services did not materialize. The impact of this has forced the security industry to reevaluate its role and develop alternatives and solutions that can be successful without a massive uptick in funding.

Business Alignment & Rebirth – The pain of the Age of Reality is now spawning the early elements of Business Alignment & Rebirth. This is a new period where security and business objectives become much better aligned and solution sets for security are deployed only where they make rational business sense. While a colossal human tragedy, the events of September 11 and its aftermath have certainly heightened all security-related activities. As a result, the stature of security within the enterprise rises from purely infrastructure overhead to business supporter.

The Path Ahead

The future will see the profession maturing and adopting a more business-like approach to security. What will get us there and continue to expand the influence and impact of security are four key drivers. By focusing on these critical areas we will solve security problems in business terms, contribute to the success of the organization, communicate in terms business owners understand, and advance the profession

Integration Ease – The security products and solutions that we deploy must have four key criteria:

1. Install easily. Lengthy multi-year implementations are not the answer any longer.
2. Be non-intrusive and operate quietly. All security solutions must be as seamless as possible and in all cases never disrupt operations.
3. Be upgradeable. We have to plan a path of flexibility. Rigid proprietary stand-alone solutions are only successful for a point in time.
4. Make a measurable difference very quickly. Security is a difficult discipline to convey true results. By identifying techniques to measure the impact of our efforts – and do it quickly – we will not only add value, but be positioned to communicate that contribution.

Cost Reduction – Budgets have been dramatically reduced in the last two years. Every initiative and budget request must be accompanied by an ROI message. This is challenging to accomplish in the security arena, but we need to pursue this goal and look to creative solutions such as outsourcing, cost re-allocation, and elimination of non-core functions.

Efficiency & Effectiveness – Security professionals have to face that they will not get every wish on their list granted. Therefore, we need to be creative and identify those controls in the preventive- detective- reactive life cycle that we can achieve. Necessity is the mother of invention and the concept could never be more valid here. There has never been a more daunting task with such limited resources.

Core Business Process Linkage – Business integration is the key to success. By becoming more strategic, we add more value to the shareholders. Study your industry alongside infosec issues. Build all your security requests in business terms and contexts. Become actively engaged with the business units – and do it early and often

So in attacking the security problem in today's challenging environment, we, as security practitioners, need to be realistic, not idealistic. We need to understand and accept that in broad business contexts, information security is viewed as overhead. Once we embrace that concept we can recognize the perception of our function and add more value. Cost reduction and ROI on all initiatives are really the cornerstones of all business and security should be no different.

****

Bruce Murphy is a CISSP and Chief Executive Officer of Vigilinx, a digital security solutions company providing practical solutions to the complex business issue of securing information.