



Peter Berlich

## Embracing risk *Peter Berlich*

Risk management has become the buzzword *du jour*. Let's put security into perspective, says Dr. Peter Berlich, CISSP, member of (ISC)<sup>2</sup>'s European Advisory Board.

**T**oday's security managers are expected to combine a thorough understanding of the technical side of IT Security with a comprehensive view of corporate compliance and proficiency in risk models with business management skills.

But in order to avoid creating gaps and becoming jack-of-trades and master-of-none, there is a clear need for more focus on where exactly those responsibilities start and end. Tomorrow's security professionals should be able to embrace the new paradigm of becoming the extended arm of business risk management.

### Where we are today

We are living in a postmodern IT world, where basic infrastructures and applications are ubiquitous and cheap. Security is just one more cost of doing business. Information theory tells us with certainty that preventing information leakage and preserving information integrity isn't free. The practical question therefore isn't just what level of security we can aspire to but what is useful and affordable.

Gone are the days of the mainframe whose security could be controlled through a single instance and which had a mature security concept. However, the perception of better mainframe security in the good old days was certainly corroborated by the fact that there wasn't today's complete reliance on IT for each and every business process.

With each new technology and business innovation, there is an incentive to defer security investments in return for affordability. The PC is a perfect example.

The fact that it was a huge step backwards from mainframe security did not hinder its proliferation - it promoted it, even when the arrival of global networks turned its apparent gaps into a ubiquitous hazard. Conversely, it is not always affordable to write off legacy systems the instant they become game for unanticipated threats.

The price we have to pay for security is artificially inflated by traditional, idealized concepts of rigid segregation. They are logical, tested and proven but do not reflect the context and culture of most modern businesses, which require flexibility and leanness above everything else.

### Changing the scope of security management

According to (ISC)<sup>2</sup>'s ISSMP (Information Systems Security Management Professional) Concentration,<sup>1</sup> a security manager will need proficiency in Security Management, Systems Development Security, Security Compliance, Business Continuity Planning as well as Law and Ethics. Similarly, ISACA's CISM<sup>2</sup> certifies the candidate to Security Governance, Risk Management, Security Program Management, Security Management and Response Management.

Within these areas, we can make out three trends that will strongly influence the way in which we will manage security in the future.

### IT risk management

The financial sector is currently in a process of aligning its risk management, driven in part by the Basel II code and other corporate governance guidelines.

Other enterprises will follow, as debtors' operational risk factors into the creditors' financial one.

IT risk managers are beginning to supplement or encompass established IT Security functions, thereby reflecting a risk management process, in which security is only one way of addressing risk. These functions need to operate closely to the business in order to be effective but their task is within the realm of a risk management function reporting to the CFO.

In order to lay the foundation for adequate risk management, a corporation will first need to take inventory of its risk posture. Since risk tends to be financially focused, it will be beneficial to think about risk in terms of business processes and focus on a limited number of identified top risks and their financial impact on the business.

Risk managers must be careful to create and maintain a balanced and flexible risk framework that is seen as an enabler, not an inhibitor to investments. In the end, it is the business manager that makes the decision. All risk management can accomplish is making the risk visible and thereby manageable.

### IT controls management

There are increased regulatory requirements for the diligent management of a company's internal risks and controls. The US Sarbanes-Oxley-Act of 2002 is only the forerunner in a global evolution of regulations and laws aimed at increasing corporate governance. Corporations with an underdeveloped internal governance posture will face significant investments and cultural change.



Based on a defined and identified risk posture, an organization will review the measures it has taken to address each risk. Where the decision has been made to mitigate the risk, IT security controls will need to be put in place. This mandates a comprehensive security policy, driving compliance throughout the corporation and down the value chain. Controls that have traditionally been seen as justified by best practices are newly being managed as part of the risk management process.

The controls function will ideally be located under the risk function or aligned with a corporate security function. Their role is crucial from a cost perspective: By defining and agreeing logical and auditable security controls the security function effectively directs the enterprise's security investment, creating a more targeted and therefore effective approach to security and improving the cost-benefit balance.

However, less is better and management must be mindful to limit the amount of rules they impose upon the enterprise. As a rule of thumb, the amount of rules an employee or an organization is able and willing to comply with can reasonably be assumed to be a constant. Consider removing one rule for each new one you create.

### IT security operations

As security breaches have become commoditized, so must IT Security operations become a commodity in order to address the security needs of the future. The provision of technical (IT) security is increasingly becoming the domain of service providers, as enterprises are focusing on their core business in order to reduce their working capital and cut cost.

The trend towards outsourcing and off-shoring of IT will enable a growing amount of corporations to delegate their operational risk to providers whose core business it is to manage security to a Service Level Agreement (SLA). This transformation will be promoted by standardization and scalable utility services.

Companies will need to retain an architecturally focused function for managing technical security standards in order to arrive at an acceptable level of technical risk. They can generate better returns and save misdirected expenses by targeting

their security investments according to their risk model.

IT security operations is where the bulk of security cost is incurred and corporations need to be constantly aware of the risks of under-investing. For the reasons described in the introduction, we are faced with a significant investment backlog in IT Security across all sectors. Risk management will help to prioritize investments in IT Security, it is not an excuse for avoiding them.

### The IT security manager's challenge

For most security managers, there is a fundamental requirement today to begin rewriting and verifying their mission statement. Any assumptions made on risk decisions need to be explicated and agreed to by management. Security managers should therefore drive for the implementation of a risk process if none exists yet.

A risk process enables us to review the enterprise's controls posture within the security domain. The effectiveness of current controls should be assessed. Some controls may need to be eliminated and others may need to be newly implemented. It will be important to maintain a sustainable level of controls.

The final element, which marks the move from a static security world to the new, dynamic world of risk managed security, is the introduction of SLAs for security controls and their elastic implementation and management.

Last not least, the security manager needs to make a mid term career decision whether she or he wants to move towards the more financially oriented world of risk management, evolve within the controls management realm or focus on technical questions.

### Conclusion

Risk management isn't the new security management; rather it is encompassing security management. The security profession has matured, and it is time for it to differentiate and embrace becoming the extended arm of business risk management instead of an embedded IT function. The CFO or the CRO, not the CISO or CSO, is the new board level function.

Highly specialized (and expensive) security technology will have its niche, but on a larger scale there will be standardized and managed security levels. Companies will have to thoroughly address their lingering problem of user compliance and sustain strong management support to their audit functions.

## IT Security operations must become a commodity

They will also have to manage their risk level instead of relying on best practice. The economic incentive is a dual one: Companies can save enormous cost by focusing their security investments and a secure infrastructure will give rise to new, flexible business models, with a just-in-time management of their computing capacity, workforce and even business processes.

1. <https://isc2.org/cgi-bin/content.cgi?category=524>

2. [http://isaca.org/Content/NavigationMenu/Security/CISM\\_Certification/Exam\\_Information1/Content\\_Areas1/CISM\\_Certification\\_Content\\_Areas.btm](http://isaca.org/Content/NavigationMenu/Security/CISM_Certification/Exam_Information1/Content_Areas1/CISM_Certification_Content_Areas.btm)

*Dr. Peter Berlich, CISSP, is working as a Security Delivery Project Executive for On Demand Data Center services at IBM Global Services on an EMEA level, based in Zürich. Before joining IBM in 2003, he was employed as global Information Security Manager at ABB, a position he held for several years. He is a member of the (ISC)2 European Advisory Board and serves on the Council of Information Security Forum (ISF). He is a member of the leadership team of German Informatics Society's section for Security Management.*

*Berlich studied physics in Kiel and Freiburg (Breisgau) in Germany. In 1997, he received an award for Internet literature from German newspaper Die Zeit and IBM.*