# Things I would not like to say about security but have to

Marcos Sêmola

## Risk

No company will be ever completely protected from the threats to its information. This would be extremely expensive or its processes would come to a halt.

Security risks and problems tend to grow exponentially and the budget for the countermeasures will never be able to keep up with them.

The compromise of information confidentiality, integrity or availability is guaranteed. The difference between one company and another is on how prepared it is are to react to and manage such a situation.

If you don't have an understanding of the acceptable risk for your business, it is best to let somebody better prepared to protect your corporate information do the job.

## Solutions

Security solutions based entirely in software and hardware are only effective temporarily, because technology changes even before they achieve their maximum level of maturity and protection.

Many years have passed, and the science of cryptography is still the basis of the most effective methods of information protection.

If your company is not visionary it will not invest in some technologies until many other companies have had sufficient negative experiences.

Security solutions need to follow the dynamism of risk agents. This is one of the reasons that technologies get outdated and only the processes last.

## Professional

To decide what should get priority is the difference between the daring and the irresponsible chief security officer.

Most security officers are corporate fire-fighters. They are not adequately positioned, and don't have the power, autonomy or sufficient resources to do a structured and integrated job in managing risks.

There is no course of any nature that will prepare information security managers. They can only be brought up by technical, managerial and human experiences.

Beware of "experts". Most of the time they are very capable technicians and students who make big mistakes on the first time they get in touch with an asset that doesn't talk, think or act in binary.

## Vendors

Consultancy companies are not truth holders, but they can help a lot by allowing you to avoid losing money and time on paths that they already know, because they have recommended them to clients in the past.

Information security consultancy companies should position themselves as financial advisers, giving recommendations to their clients on how better to invest their capital considering the individualities of their risk profiles.

There is no methodology, tool, training or procedure that makes the consultancy business scalable. On the day that this happens, we will all be buying and selling something else.

Theoretically, the vendor that gathers all the components of a security solution but can sell it in small chunks is the one which is better prepared to help companies which have distinct levels of risk management maturity.

...

## Conclusion

Theoretically, we will achieve the adequate security maturity level when we are not able to notice it anymore. It can be said that the security process is going well when nobody remember it exists. But if the processes are stuck, the users are unhappy because they have to change their passwords more often than they change clothes and the chief executive is questioning why, despite all the investments in security, he still receives more spam than e-mail, then something is wrong, very wrong.

*Marcos Sêmola is a certified infosecurity professional, MBA professor and author (**web-site**). Until November he was head of information risk operations for Atos Origin in the UK.*



http://www.infosecurity-magazine.com/comment/071109_semola.htm