Article number 65 published in March 2005

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

Risk

- No company will be ever completely protected from the threats to its information. This would be extremely expensive or their processes would come to a halt.
- The security risks and problems tend to grow exponentially and the budget for the countermeasures will never be able to keep up with it.
- The compromise of information confidentiality, integrity or availability is guaranteed. The difference from one company to another is on how prepared they are to react and manage the 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 it.

Investment

- Shareholders and executives have to identify and realize the return to invest in security, there is no other reason that will get them out of the inertia.
- Experts have been looking for ROI formulas to mathematically justify the investments in security for a long time, they won't stop anytime soon.
- Specific legislation, general and sector regulation and internal and external audit are, to the moment, the most effective motivational instruments for investment in information security
- Apart form that fact that the Paretto 80/20 rule also applies to information security, if you have only "one pound" to invest in security you should give up. You won't be able to do anything effective with so little.

Compliance

- ISO 17799 standard is not the solution to the information security problem, but it is a guide full of advice which facilitates the conversation between technical personnel and executives from different companies.
- The references ISO17799/BS7799, COBIT, COBRA, ISO13335, ISO15408, ITIL and other, will only be a list of acronyms that generate work and cost if they are not applied to the reality of each business.
- To follow the ISO 17799 recommendations verbatim may not lead your company to the adequate security level, but you become less liable since everybody is following the same direction

- North American law Sarbanes Oxley is, no doubt, the newest and most effective factor to motivate compliance, after all who is under threat is the budget owner.

People

- The security attitude in the user behavior is proportional to the ease of use and the negative consequences to the user's career.
- The human being is the only asset is the risk equation that lasts to the test of time and can evolve cumulatively without the need of expensive upgrades
- Any security process is as safe as the security offered by the human asset that it is composed by.
- People are naturally different in their preferences, its wills and their values. Because of that every security solution should identify the motivational factors of every group to transform them in agents and not threats.

Solutions

- Security solutions based entirely in software and hardware are only effective temporarily because technology change even before they achieve their maximum level of maturity and protection.
- Many years have passed and the science of cryptography is still the base of the most effective methods of information protection.
- If your company is not visionary it won't invest in some technologies until many other companies had sufficient enough 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 CSO.
- Most of the Security Officers are corporate firefighters. They are not adequately positioned; don't have the power, autonomy and sufficient resources to do a structured and integrated work to manage the 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 don't talk, think or act in binary.

Vendors

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

- Information security consultancy companies should position themselves as financial advisories, giving recommendations to their clients on how to better invest its capital considering the individualities of its risk profile.
- There is no methodology, tool, training or procedure that makes the consultancy business scalable. In 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. In a few words, 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 CEO is questioning why, besides all the investments in security, he still receives more spam than e-mail, than something is wrong, very wrong.

Marcos Sêmola *is Head of Operations of Security & Information Risk at Atos Origin in London, United Kingdom, Senior Consultant of Information Risk Management field, CISM - Certified Information Security Manager, BS7799 Lead Auditor, member of ISASA, ISSA, IBCG, CSI and further founding member of IISP – Institute of Information Security Professionals of London. Post Graduate in Negotiation and Strategy, MBA Professor of Information Security Management at FGV Business School, Master in Business Administration with Applied Technology in Business, Bachelor in Computing Science, author of the book Information Security Management - The Executive View by Campus publishing house, co-author of the business book Information Strategy Management & Competitive Intelligence by SaraivaUni publishing house and also co-author of the academic book Information and Communication Technology. Awarded the SECMASTER®, Information Security Professional of 2003 Private Sector and 2004 Market Development in Brazil by ISSA - Information System Security Association and was invited member of Award Academy in 2005. Visit www.semola.com.br or use marcos@semola.com.br*