77 – July 2006

In security of information, less may be more.

Simplifying has been my challenge in the past 7 years, writing and speaking about information risk management in lessons and lectures. I believe that companies and *Chief Information Security Officers*, in general, should channel their efforts and focus on dealing with more relevant threats and risks, and thus, invest time and money in the most significant of problems. This approach does not reveal anything new, but at times we do not regard them as coherent and practical behaviour, if we keep thinking so, and even before old and familiar problems are resolved or definitely dealt with, we immediately grab them and go on thinking and looking for new problems to resolve.

Once more Pareto's concept seems to apply and tells us that, almost certainly, 80% of the problems are managed with only 20% of effort. I may be very wrong and my simplification exercise completely wasted in the near future, but for me, in this case Less could mean More.

What I am trying to say does not ignore the evolution and dynamism of threats, failures and incidents, but is based fundamentally on the perception that many of the security problems are conceptually common to every business and are still real, despite being many times, treated as old-fashioned problems that do not deserve or detain the attention of the information security professionals. Momentarily, the security segment seems to follow the movement of the high technology market or the fashion market, where techniques and products become old and outdated by the simple emergence of something new. The outcome is disorientation and the inconvenient enthusiasm for new projects, without knowing if the former ones had been successful.

Refresh your memory and make up a list of security problems and incidents that have been identified in your company in the last few months. Now, imagine how this list could have been different if some of the older problems related to password, access permission, updating system, virus, content control, classification of documents, backup, segregation of network and removable media had been resolved, or at least had been administered more readily. Well, this is exactly what I am referring to.

I cannot deny the importance of tailor-made security, nor all the potential controls and necessary processes to sustain the operation of a complete system of information security management, promoting the increase of maturity and control levels. However, it does not seem coherent to me to worry about modern problems while the old and familiar ones remain unassisted. I do not see it as a wise decision, for example, if there are financial and temporal limitations, spending the small budget on an ambitious identity management project while the profiles of access are left without segregation and the passwords without a strong policy.

In practice, I ask myself, for example, why is there a long risk analysis project to identify and classify the potentially long list of vulnerabilities if many of them are previously known and are sufficiently complex to take up all the time of your team and your budget? Why mobilize the *stakeholders* and representatives of key areas of the company to write a security policy if there are known guidelines and readymade norms that can be immediately incorporated by means of one adaptation or another, without much effort and with high effectiveness? Having this in mind, I have suggested this brief list of actions:

• Define rules and a structure for the management of access passwords. Try to find solutions that allow the cancellation and renewal of the password by the users themselves. In addition, improve the model of segregation of functions, profile definitions, remote access, monitoring and auditing authorised access, including the resources of the operational system. Together, these factors are responsible for a large part of the problems related to unauthorised access and loss of information due to human error.

• Classify the information and define rules of conduct for using, storing, transporting and discarding it in the physical and digital formats. Without these parameters and their knowledge, anyone who could be an ally of security cannot help, and whoever could offer risk will not even acknowledge the fact of being non-compliant with the policy.

• Segregate your data network physically and logically based on classification of information and requirements of access to applications and services. Project possible scenarios of unauthorised access, unavailability, and especially contamination by virus. This effort will be rewarded by a more intelligent network both in the proactive monitoring of threats and in the reactive administration of incidents. Just as it happens in a building, if the piping system for water distribution and the segregation through the mains are intelligent, a simple leak in one of the rooms on a specific floor will not interrupt the supply to all the other residents.

• Invest in solutions of intelligent and compatible backups with the sensitivity of information and the business. Clearly define the backup processes, document them, often test them and train the operators, because both human failure and intentional and natural threats are responsible for a significant part of the business interruptions and impacts.

• Establish procedures and a management routine for security updates using the current management structure. The time gap between the discovery of vulnerability and applying a corrective measure will determine your level of exposure to risk. Even so, do not plan a reactive structure D+0 or D+1 too soon, at first, because this decision may require high investment, while the simple decision of creating a *patch management* process will already place you at another level of security.

• Concentrate a large part of your energy on the control strategy of malicious content, virus and in the control of removable media. Implement a corporate antivirus solution not dependent on the user interaction, guaranteeing the environment-oriented update and cleanup. Internet-accessing filters and the control of removable storage devices may considerably reduce the problems of information leakage.

www.semola.com.br marcos@semola.com.br

Simplifying:

1. Define criteria for the creation and renewal of access passwords
2. Segregate profiles and authorised access to the systems
3. Segregate the data network physically and logically
4. Limit the access to operational system resources
5. Limit the use of removable devices
6. Implement an antivirus and content control solution
7. Implement a security update management solution
8. Classify the information and define handling procedures
9. Document and test backup routines periodically
10. Adopt security policies for the themes mentioned above and train users

Also like a realignment handle, accept the need to follow the results of the 10 actions to assess the return, extract lessons learned and promote continuous improvements. I am sure that it has been a good and consistent start.
And remember: what you do not know you cannot control. What you cannot control you cannot measure. What you cannot measure you cannot manage, and what you cannot manage you cannot improve.

Marcos Sêmola *is Business Development Consultant of the multinational company Atos Origin in London, Senior Consultant in Information Security Management, Professionally certified CISM – Certified Information Security Manager by ISACA, BS7799 Lead Auditor by BSI, Member of ISACA, ISSA, IBGC, CSI and founder of IISP – Institute of Information Security Professionals of London. Professor at FGV – Fundação Getúlio Vargas – with specialisation in Negotiation and Strategy by London School, MBA in Applied Technology, Postgraduate in Marketing and Business Strategy, Bachelor in Computer Science, author of the book Information Security Management – an executive view, Ed. Campus, author of two other books on information management by publishers Saraiva and Pearsons and awarded by ISSA as SecMaster®, 2003/2004 Information Security Professional, as a member of the judging committee in 2005. Visit www.semola.com.br or contact marcos@semola.com.br.*

N.B.: This article expresses exclusively the personal opinion of the author, and does not represent necessarily the opinion of the company mentioned.

Translated by Global Translations.BR - www.globaltranslations.com.br