76 – June 2006

Does Security halt or accelerate business?

Finally, when information security was no longer an issue restricted to basement headquarters, to intelligence and counter-intelligence development studios and was present in board meeting rooms, at the desks of auditors, administrators and security officers, confusion had already been formed.
What was born with the legitimate and unidimensional purpose of protecting the confidentiality of communications has been transformed, following the requirements of a new business world and, thus, has taken on multiple applications and dimensions. The speed with which this has been occurring associated with the enthusiasm of those who want to spend a lot of time on the clipboard, reviewing and revalidating concepts or, simply, opposing them trying to find methodological innovation, increasing the confusion.

I think that many of those that are getting involved and have decided to "do" information security do not know it in its essence. It is likely that they have a correct view, yet isolated and focused on the problem that is within the reach of their eyes, and not necessarily an integrated view of the inherent, present and residual risks and thus, the real perception of the implications and reasons to "do" information security. Everything should work like an orchestra where every musician dominates and knows exactly what to do with their instrument, but only the conductor has an overall view and is able to coordinate isolated actions in search of one result that captures the original essence of the masterpiece.

It would be ingenious to think that the current multidimensional challenge of protecting confidentiality, integrity and availability of information would be clear at all levels of the hierarchy and at all the activity layers, that one would entirely understand the importance and methods of data transmission, layers of protocol, session keys, cryptographic algorisms, wireless networks, operational systems and all their versions, the development techniques of secure applications and their interfaces. And that, in addition that one would see physical aspects, segregation of perimeters, audit sensors and trails, contingency, policies and procedure, as well as all the other implications resulting from human, market-related, financial and legal aspects that inevitably surround their orbit.

Like any other product or service that is known, information security also has a crucial purpose and this should be clear. For complex products and services, as it happens here, it is necessary to understand the purpose of each activity layer to know the essential purpose.
Let us take for example the installation of a backup system in a financial institution. While this action has the first level purpose of automating the production of security copies to guarantee the maximum availability of information because of the loss of the main storage media, the second level is to increase adherence to the company's backup policy. This one, in turn, adheres to the purpose of the third level to guarantee compliance with external sectorial audits, until finally proceeds with the essential purpose of being recognisably a company that offers high value products and services be it through its reputation in the adoption of best practices or simply by means of its effectiveness in crisis situations faced

previously. Information security in general, was the instrument of valuation of the business and brand, and increased the perception of value.

In the market in general and in this case in particular, information security offers controls that in analogy with a vehicle, represent the brakes. However, different to the initial interpretation, which we made regarding the brakes of a vehicle, this is not intended to prevent the car from going any faster. On the contrary, the efficiency of the brakes is the key component considered so that motor engineers can develop even faster vehicles with the certainty that they will stop efficiently in a moment of crisis. In practice and speaking "businesswise", having effective mechanisms of information risk management is being apt to be daring, innovating within the level of risk considered acceptable. It means being confident to impose higher speeds to the business, to diversify, and offer new tools and methods of work that finally support the essential purpose of adding value.

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, 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, becoming a commission member in 2005. Visit www.semola.com.br or contact marcos@semola.com.br.*