58 – June 2004

Information Security to protect the Manager

Protecting important information for the company's operation, does that make any sense to you? In addition, what about protecting the information in order to protect the manager? Now, more than ever, yes. The last of the three factors that encourage investment in information security, liability, is beginning to make sense to companies and to the people who are running business.
Besides keeping themselves motivated by the need to make it and not lose money, complying with laws, national and sectorial regulations and global norms have had more influence in the process of deciding on investments.
For a long time some sectors of the economy have suffered the incidence of their own operational rules, the requirement of standardised service levels and the maintenance of controls that support frequent audits performed by regulating bodies.

The financial segment is an excellent example of this. Besides the financial institutions and other institutions authorised by the Brazilian Central Bank having to adopt numerous mechanisms to guarantee the existence and maintenance of internal controls – like periodic security tests for information systems – pursuant to Resolution 2554, they also have to guarantee operational redundancy for the availability of services, pursuant to Resolution 2892, to regulate the processes of operating deposit accounts exclusively by electronic means pursuant to Resolution 2817, to adopt, among other things, strong cryptographic mechanisms for access and exchange of information within the Brazilian Payment System (SPB) and also to be in compliance with the criteria and risk management procedures defined globally by the latest edition of the Basel Agreement.

Like in the financial sector, other sectors of the economy are also influenced directly by national and sectorial regulations that create the need for new information security controls and mainly, if they are not respected, create liabilities in the form of fines.
It is exactly at this point that the managers take on their role, because the modern concepts of corporate governance associated with the new Civil Code, which increases the responsibility of the administrators, and also influence the Sarbanes-Oxley Act, which predicts, among other things, the communication of the personal effects of managers in situations of compromised credibility of companies they are administering, makes them motivated and potentially liable for the poor management of information risks.

Commitment to the efficiency of internal processes, development of new business, reduction of costs, extension of market share, or simply bottom line balance sheet figures are no longer sufficient to guarantee the efficiency of managers. It is necessary to demonstrate commitment and maturity in the management of risks, in the preservation of information and, consequently, in processes supporting the results. It is necessary to be in compliance with rules, and by doing so remain free from corporate liability that can be extended to personal liability.
In addition, everything makes us believe that there is no longer organizational segregation in companies that isolate concerns with security aspects. What was once a limited matter in

the more technical and operational forums, therefore the base of the corporate pyramid, has completely escalated and reached executives and managers. Now, security does not only protect information and the operational continuity of the company, it also preserves the financial health and the professional future of its managers.

Marcos Sêmola *is Security Consulting Manager at multinational company Atos Origin, Senior Consultant in Information Security Management, CISM – Certified Information Security Manager, Professor of Information Security at FGV – Fundação Getúlio Vargas, MBA in Applied Technology, Bachelor in Computer Science, author of Information Security Management – an executive view, Ed.Campus and elected for the SecMaster award, Information Security Professional of 2003.*
Visit www.semola.com.br – 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.