57 – April 2004

Motivation: the key to security

Protect information that subsidises the operation of the company's business processes. Reduce and administrate the information risks and the impacts potentially provoked by an incident of leakage, fraud, sabotage and unavailability. These seem to be the main reasons that lead the executive and his consultative committee to adopt measures and make security investments, but it is wrong to think so.

If it is at the strategic level like the sphere of the CEO, CIO, and CSO or at the tactical and operational levels, any initiative should be supported by a motivational factor. Something that will make them leave inertia aside and do something about it.
The motivation is inside us and is responsible for any of our actions. The decision to purchase life insurance, to avoid a cinema session after 11 p.m., or simply a decision to put your seat belt on, or not, in the car is, despite being imperceptible at first analysis, associated to some motivational factor.

Thus, we could be fooling ourselves – like many do – thinking that the executive body decides to invest in information security following the market trend, to be recognised as visionary, ahead of competitors, not behind them, to avoid losses that others have already had, to avoid repeating losses you have already suffered, to strengthen your image of credibility through marketing, or also, to be in compliance with sectorial regulations or laws. In reality, when they only think – objectively – about the three reasons or factors that motivate them: making money, not losing money and not being liable.

There is nothing else that will make them adopt an attitude, except think about the profitable development of their business and the administration of their responsibilities that involve the management of a company. These responsibilities are based on modern concepts of corporate governance under the Sarbanes Oxley Act.

Now, we have seen why the motivational factor is important. Nevertheless, we need to understand that information risk management is not only done as an initial investment, nor as isolated planning. We need to cover the strategic, tactical and operational spheres, besides finding the specific motivational factors for each level of the chain. If the CEO has found motivation to invest in a corporate mechanism to control physical access, we need to find and materialise similar motivation for the CSO, Directors, Managers and also the end user. Without this, chances are that the results of the project may not create the desired effects, and the consequent return on investment will be discouraging, not likely to become a continuous process over time.

If there is a lack of any motivational link, the corporate chain of security management will not be appropriately structured and will come apart.

In a brief exercise, we can say that the Investor is motivated by the increase of the investment, while the CEO is motivated by the business results, the CFO is motivated by the credibility of information, the CIO by the effectiveness of services, the CSO by the efficiency of risk management, the Director by the productivity of processes, the Manager by the productivity of the employees, and last of all, the User by factors inherent to their end activity.

What to me seems like the secret of success of any security initiative, be it comprehensive, or not, is to identify the specific motivational factors of each element of the subject involved and make it tangible and familiar, so that they can then fulfil their role and close the cycle that will give life to another process in the risk management framework.

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