60 – August 2004

Pareto and Security

Pareto, an Italian scientist, discovered in the last century, a cause effect relationship in which 80% of the results are generated with an effort of only 20%. It may seem unreal, but the time and continuous exercises with the figures have shown managers that 20% of the salespeople of a company generate 80% of the sales; 20% of the clients are responsible for 80% of the revenue or that 20% of the rural producers of a city generate 80% of the production.
The importance of Pareto for Security is associated with the large dimension of effort necessary to continuously reduce and administrate information risks. Despite physical, technological, human and processing vulnerabilities increasing and being renewed daily, the amount of investment compatible with the asset to be protected, or simply available, is finite.
This limitation is real and the problems are more than heterogeneous, therefore, the large current challenge of Chief Security Officers and specialised Consultancy companies is the support structure in the decision process that will define what should be postponed, what should be given priority to and even, what should be forgotten and disconsidered in the investments.

It is undoubtedly a difficult situation, but the blind search for theoretic excellence only based on international norms and best practices should give in to the prioritised management need based on the interests of the business. The act of investing in information security should be conducted with the same seriousness as an executive deciding on extending their production line or automating their sales force, i.e. with the results in mind.

It does not make any sense investing in time, money or resources of any nature, that are worth more than the asset being protected. It does not make sense carrying out actions in long security analysis processes if they cannot guide you into correcting failures swiftly. It does not make any sense putting effort into obtaining the BS7799 certification, for example, if the greatest problems that compromise confidentiality, integrity and availability of your information continue being viruses, the Internet perimeter, your electric infrastructure and the conduct of your employees. It is like preparing a vehicle for a journey that will take 2.000 km installing spare tyres, cruise control, spare parts for the engine and GPS, and forgetting to fill the tank with fuel.

Pareto's Principle should direct security and consultancy executives, because time and money are finite, but the problems are not. Deciding on what should have priority, what is more representative for the nature of the business, assessing what is more relevant, contextualising the failures and identifying the actions that represent the 20% effort that will be responsible for 80% of the results.

Intelligent investment is the key that can lighten the burden of investments that cannot be measured, of projects that will generate only attractive and solid reports, of the inconsistent search for certification, of the solution only academically perfect and the specification of ready-made and utopian security policies. Even when applied to security, we are speaking about investments that, like in any other situation, should be directed towards the interests of the business and its managers, allowing for the generation with more money to reduce losses and liability risks.

Considerations to support the decision process and maximise investments in information security:

• Consider the requirements of the business (nature of activities, sensibility, tolerance and criticality);

• Consider the short, medium and long-term business plans (development and investment plan);

• Consider the relevance of the processes for the business (direct and indirect relationship with the financial results);

• Consider the perception of priority of the information assets (dependence on the business processes);

• Consider the technical, temporal, financial and legal limitations and other specific limitations (sectorial regulations, Constitution, technological platforms, etc.);

• Consider the inherent risk, present risk and residual risk (predictable risk configuration, current risk and final or desirable risk);

• Consider the current and desired situation (level of ideal security for the context of the business: compatibility of investment and tolerance), and

• Consider the model of maturity (following indicators and measurement of results to retro feed the risk management process).

Marcos Sêmola *is SAM 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, 2003 cat.4, Information Security Professional.*
Visit www.semola.com.br – marcos@semola.com.br

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