Free distribution if the source and author are mentioned

69 - October 2005

Security will be jeopardised, it is just a matter of time.

This is another commentary on the series that explains and tries to illustrate each of the statements of the article "Things I would not like to say about security, but I have to".

> "Breach of confidentiality, integrity or availability of information is certain. The specific difference between one company and another is the way in which they are prepared to administrate and react to a situation. "

It is almost a mathematical statement, for if there are failures and threats, therefore risk, the resulting impact of the exploitation of the former by the latter is certain, and it exclusively depends on time. It is very likely that at some point security will be breached, in one way or another, and the efficiency of your risk management process in response to the incident is what will determine its quality.

Many companies, which in the eyes of the market and of your client are solid, 'protected' and immune to information attacks, are in fact being competent. Not in being surrounded by all mechanisms to eliminate the risk, but competent in the good daily management of security where the clients do not even notice their occurrence. It is as simple as that.

Once again, using the automobile model to make things clear, we can make an analogy comparing a high-speed race like the Formula One with a certain problem. The cars that participate in a race like this one, in which all the components will be tested to the extreme, there is only one expectation: to break down. Breaking down is the most predictable factor. I am obviously not speaking about fatal breakdowns in which the car does not even reach the pits, but the small breakdowns that can take precious time off pilots and that can be administered during pit stops.

The nature of the activity already presumptions the existence of potential problems in the racecourse, the same that happens to a company that decides to use the public Internet network to support its model of e-commerce. The difference and competence of both is measured by the way in which they respond to incidents, how they repair the split aerofoil without interrupting the race, or the overloaded network link by a new computer virus without interrupting sales on the web portal.
To achieve this task effectively it is important to experiment situations, build scenarios, and simulate actions and reactions to the problems, when they appear, being them familiar or previously studied so that only the steps of mitigation or recovery need to be followed.

The exercise of predictability is fundamental, but not just the technical exercise in which problems and possible solutions are studied, but also tactical and strategic exercises.
It is equally important to know if the car will continue in the race or if it is not possible to repair a part, because it can be quite risky for the business to make this decision or it may be simply strategically important to let it go on.

Being practical, the analysis could follow this train of thought: could the part be replaced or repaired in time? If so, replace or repair the part. If not, will the broken part put the pilot’s life at risk? If so, interrupt the race. If not, will the car be totally jeopardised? If so, what is the value of the car? Is the financial tolerance able to accept the loss of the car? If not, is it worth running the risk of losing the whole car so the pilot can do the last lap and win the championship, generating enough profit to purchase 3 new cars? If not, interrupt the race. If so, go ahead and good luck.

All this process may seem a bit much for some companies, but in fact, this method can be applied to any company, any activity, and any business model and can even be applied to the domestic computer user. Think of your computer, a *notebook*, for example, as an important tool used to pay accounts over the Internet, to carry out master degree assignments, to store photos of the family and produce your first romance. Now, think of the possible loss of your hard disk, where everything is copied and gives you a false sense of security and makes you think that everything is safe and accessible at any time.

Well, without consulting the stars or resorting to divination it is possible to affirm that one day you can lose the documents stored on this disk. It is true. It may be through a defect in the computer, it could be dropped, hit by lightning, short-circuited, a large cup of soda spilt on the keyboard, a theft, affected by a devastating virus or simply the user could accidentally delete the content, and you *will* lose everything. At this moment, the way in which you exercised predictability will determine the result. Can the part be replaced or repaired? If not, is there an alternative to recover its content? If so, restore the backup. Congratulations! If not, be prepared next time, and start from scratch.

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 and Computer Security Institute, 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, and awarded by ISSA as SecMaster®, 2003/2004. 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