73 – March 2006

Predictability Factor

The predictability factor is very important in information security, especially in environments with low tolerance towards failure. Like what happens in critical activities like the Olympic Games, many other corporate activities, environments and processes detain the same sensitivity, and for this reason they need to develop and maintain mature predictability mechanisms so they are better prepared to face a situation of crisis. Being prepared does not necessarily mean avoiding a risk or preventing the impact, but to recognise its probability and have alternative procedures to minimize its severity and its extension, guaranteeing minimum conditions of survival and continuity.

As the tolerance of the environment decreases the quality of what is predictable should increase. There are many ways of measuring tolerance, simple or complex, but the unit of time is applied in the majority of cases and makes it easier to understand. If we consider, for example, the environment of a TV assembly line and we compare it to a hospital surgery, we will certainly detect clear differences to tolerance. Equipment for image tube testing that is not working properly can, conceptually speaking, wait several minutes before being repaired or can be replaced without any damage or impact to the business. On the other hand, a breathing apparatus that is not being used during surgery cannot wait more than a few seconds to be replaced or go back into use, without causing any damage. This example may be considered extreme because it involves human life, but it is clear enough for everyone to realise that tolerance is related to the capacity of the environment absorbing the impact and surviving it without any significant damage, or simply, within a level of tolerable damage.

Possessing the attribute of predictability is to maintain dynamic processes that analyse, develop, document and maintain the scenarios of updated studies. From the definition of potential threats, feasible by the nature of the environment, the action of each of the threats is projected into each of the resources of the environment, tracing the potential impact in terms of severity. The first result of the exercise is a multidimensional matrix associating threat, resource, impact, severity, recovery time, tolerance of the resource in relation to the nature of the environment and the recommended procedure. In practice, after the procedures have been adequately documented, they should be used as guidance for the environment users when facing a situation of crisis.

The quality and amplitude of the scenarios should be directly proportionate to the tolerance of the environment. Imagine the diversity of potential problems on a flight. Match threats, resources that support the aircraft operation and its tolerance. If an aircraft presents any problem in the landing gear, for example, its solution should be on board. In general, the tolerance to the problem is low, because the fuel is limited forcing the aircraft to land somewhere at a certain time. That is why all possible situations of crisis with the landing gear have to be considered and documented beforehand and should guide the air crew so they can react quick and precisely. In general, there is only time for diagnosis, to assess the

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

extension of damage, to consult the procedures to identify the exact situation diagnosed and then follow the recovery or contingency procedure step-by-step.

Situations of crisis are extreme *per se*. Components of nervousness, inexperience and the complexity of the problem itself become worsening factors, and that is why everything should be thought about in advance: the place where the crisis procedures are stored, going through the documentation format, the words used to describe the problem and even the size of the font used in the text should guarantee appropriate reading in adverse conditions. Time, as mentioned is a critical factor and reaction should occur within the tolerance span of the resource affected. Depending on the context, there could also be sub levels that consider the potential failure of the first contingency procedure, triggering a new level of procedure, until the problem is effectively resolved. It is indispensible to say that the phase of tests is crucial to refine and guarantee operational adherence to the procedures.

Predictability, therefore, has nothing to do with card games, divination and crystal balls, but with the quality of what is predictable from the perception of risk and tolerance. Exercising predictability is natural and healthy. It means being prepared for problems that are still inexistent. And this no doubt will determine the success or failure of your company in the next situation of crisis.

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, author of two other books on information management by publishers Saraiva and Pearsons 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