76 – Junho 2006

Segurança freia ou acelera os negócios?

Quando finalmente a segurança da informação deixou de ser um assunto restrito os porões dos quartéis generais, às oficinas de desenvolvimento de inteligência e contra-inteligencia e chegou às salas de reunião de diretoria, à mesa dos auditores, administradores e security officers, a confusão já estava formada.
O que nasceu com o propósito legítimo e unidimensional de proteger a confidencialidade das comunicações, foi se transformando, acompanhando os requerimentos do novo mundo dos negócios e, assim, assumindo múltiplas aplicações e dimensões. A velocidade com que isso vem acontecendo associada ao entusiasmo dos que querem realizar sem despender muito tempo na prancheta, revisando e revalidando conceitos ou, simplesmente, contrariando-os a fim de buscar inovações metodológicas, aumentam a confusão.

Penso que muitos dos que hoje se envolvem e se propõem a "fazer" segurança da informação, não o saibam em sua essência. É provável que tenham uma visão correta, porém isolada e focada no problema que está ao alcance de seus olhos, e não necessariamente uma visão integrada dos riscos inerentes, presentes, residuais e assim, a real percepção das implicações e das razões para se "fazer" segurança da informação. Tudo deveria funcionar como em uma orquestra onde cada músico domina e sabe exatamente o que fazer com o seu instrumento, mas só o maestro detém a visão do todo e é capaz de coordenar ações isoladas em busca de um resultado único que capture a essência original da obra.

Seria ingênuo pensar que agora o desafio multidimensional de proteger a confidencialidade, integridade e disponibilidade das informações estivesse claro para todos os níveis hierárquicos e em todas as camadas de atividade. Que compreendessem em sua plenitude a importância e os métodos de transmissão de dados, camadas de protocolo, chaves de sessão, algoritmos criptográficos, redes sem fio, sistemas operacionais e todos os seus "sabores", as técnicas de desenvolvimento de aplicações seguras e suas interfaces. E que, além disso, ainda enxergassem os aspectos físicos, a segregação de perímetros, os sensores e trilhas de auditoria, a contingência, políticas e procedimentos, bem como todas as outras implicações advindas de aspectos humanos, mercadológicos, financeiros e legais que inevitavelmente giram em sua órbita.

Como qualquer outro produto ou serviço de que se tem notícia, a segurança da informação também tem um propósito essencial e este deve estar claro. Para produtos e serviços compostos, com o que ocorre aqui, é preciso compreender o propósito de cada camada de atividade para finalmente conhecer o propósito essencial.
Tomemos como exemplo a instalação de um sistema de backup em uma instituição financeira. Enquanto esta ação tem o propósito de primeiro nível de automatizar a confecção de cópias de segurança para garantir o máximo de disponibilidade da informação diante da perda do meio de armazenamento principal, o segundo nível é o de aumentar a aderência à política de backup da companhia. Este, por sua vez, adere ao propósito de

terceiro nível de garantir a conformidade com auditorias setoriais externas, até que finalmente, toca o propósito essencial de ser reconhecidamente uma companhia que oferece produtos e serviços de alto valor. Seja por sua reputação diante da adoção de melhores práticas ou simplesmente por sua eficácia diante de situações de crise vividas anteriormente, a segurança da informação de uma maneira geral, foi o instrumento de valorização do negócio, da marca e aumentou a percepção de valor.

No mercado em geral e neste caso em particular, a segurança da informação oferece controles que analogamente a um veículo, representam o freio. Contudo, diferente da interpretação inicial que fazemos do freio para um veículo, este não tem o objetivo de impedir que o carro ande mais rápido. Ao contrário disso, a eficiência do freio é justamente a peça chave para que os engenheiros de motores possam desenvolver veículos ainda mais velozes com a certeza de que estarão prontos para parar eficazmente diante de uma situação de crise. Na prática e sob a ótica dos negócios, possuir mecanismos eficazes de gestão de riscos da informação é justamente estar apto a ousar, a inovar dentro do nível de risco considerado aceitável. É estar mais confiante ao impor velocidades maiores ao negócio, ao diversificar, e oferecer ferramentas e métodos novos de trabalho que finalmente suportem o propósito essencial de gerar valor.

Marcos Sêmola *é Consulting Business Development da multinacional Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, profissional certificado CISM – Certified Information Security Manager pelo ISACA, BS7799 Lead Auditor pelo BSI, Membro da ISACA, ISSA, IBGC, CSI e membro fundador IISP – Institute of Information Security Professionals of London. Professor da FGV – Fundação Getúlio Vargas, Pós Graduando em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed. Campus, autor de outras duas obras ligadas à gestão da informação pelas editoras Saraiva e Pearsons e premiado pela ISSA como SecMaster®, Profissional de Segurança da Informação de 2003/2004, sendo membro da comissão julgadora em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br*