

48 – Junho de 2003

## Qual o papel do Gestor de Segurança?

De acordo com um estudo da Giga Information Group de março deste ano, embora os departamentos de segurança da informação de corporações do mundo todo tenham recebido um aumento médio de 5% em seus orçamentos, mais de 50% das empresas investiram em projetos de segurança incorretos e irrelevantes. Além disso, a Giga prevê para este ano, que mais de 90% de todas as organizações nomearão um indivíduo ou um departamento especial para esta tarefa de gerir a segurança da informação.

É certo que esta última previsão motivadora é um sinal de amadurecimento das empresas quanto ao tratamento dos riscos e a percepção de relevância de um processo estruturado de gestão. Contudo, poucos profissionais têm a clara noção dos desafios e principalmente do papel desse gestor. Por vezes, o simples título Security Officer ou CSO – Chief Security Officer presente no cartão de visitas, pode conduzir a um entendimento distorcido da realidade, pois esta posição costuma apresentar grandes diferenças de atribuição e autonomia e assim, reflete diretamente a estrutura organizacional da cada empresa.

Atualmente, o mercado reúne empresas que vivem os mais diferentes estágios de administração de riscos e segurança da informação. Começando por aquelas que simplesmente desconhecem o problema e tão pouco julgam prudente investir – na percepção delas, gastar – dinheiro com recursos específicos. Em seguida aparecem as empresas que já sofreram prejuízos com a falta de segurança ou iniciaram um processo de conscientização interno ainda baseada em ações tecnológicas. Penso que este segundo grupo corresponde à grande fatia do mercado pela simples falta de visão dos executivos na mensuração dos riscos e do retorno sobre o investimento. Além dessas, uma porção muito seleta de empresas se encontram em fase mais madura, dimensionando investimentos com abrangência corporativa, integrando ações que visem a tecnologia, os processos e as pessoas, e ainda levando o assunto para discussão em comitês executivos e alta gerência.

É bem verdade que não podemos classificar o universo de empresas em apenas três níveis de evolução, mas estes já nos dão um panorama para compreender as dificuldades em se definir um responsável pela segurança da informação e principalmente estabelecer suas responsabilidades e competências necessárias para que os objetivos maiores do negócio sejam atingidos. Neste momento cabe uma pergunta: qual o papel do gestor?

Em linhas gerais, o CSO ou Security Officer tem que ter um perfil executivo, tomando partido das decisões macro-estratégicas da companhia e participando ativamente da modelagem do plano diretor de segurança da informação, um instrumento de orientação abrangente e intimamente alinhado ao ROI e aos interesses do negócio da empresa.

Por analogia, este profissional seria o maestro de uma orquestra preocupado em compor os membros da equipe (própria ou terceirizada), garantir o ritmo, as metas de desempenho, as integração das ações, a interoperabilidade entre as cordas, os metais, a percussão – como se

fossem departamentos de uma empresa - e principalmente a harmonia em cada atividade programada.

Falando mais especificamente sobre o perfil, o profissional deve possuir uma formação generalista com experiências que cubram o espectro técnico e gerencial. É certo que por inúmeras vezes estará diante de desafios e atividades demandadas por problemas em ativos tecnológicos, porém, toda e qualquer decisão que tomar deverá estar sustentada pela percepção clara de suas funcionalidades para com os processos que efetivamente adicionam valor ao negócio da empresa. Deve ter habilidades de liderança e relacionamento interpessoal bem apuradas por ter de ser um articulador presente na integração de departamentos, gestores de outras áreas importantes. O puro domínio da tecnologia, demonstrado comumente pela obtenção de selos e certificações, perdem importância se o mesmo não possuir uma visão prática de aplicabilidade. Neste caso, é melhor contar com profissionais reconhecidamente especializados e continuamente capacitados, em sua equipe.

Diferente do que muitos imaginam, este gestor não deve se sentar simplesmente na cadeira do comprador de produtos e serviços de segurança, mas atuar de forma comprometida com os resultados da empresa, por exemplo: metas de performance de processos; metas de retorno dos investimentos; metas de risco; metas de confiabilidade e continuidade do negócio etc.

Diante dessa situação, seria muito confortável estar de posse dos melhores livros, normas, cases e recursos físicos, tecnológicos e humanos, para implementar todos os controles aplicáveis e necessários para que a empresa atinja o nível de segurança controlado. Entretanto, essa situação não existe. Tempo e dinheiro são finitos, portanto, precisam ser bem empregados em ações igualmente bem priorizadas para produzir o maior resultado possível com o menos investimento. Esse deveria ser o papel do verdadeiro gestor.

*Marcos Sêmola é Consultor Sênior em Gestão de Segurança da Informação, Professor de Segurança da Informação da FGV – Fundação Getúlio Vargas, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação e autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed. Campus 2003. Atualmente é Consulting Manager da Schlumberger Worldwide IT Partner..*  
[marcos@semola.com.br](mailto:marcos@semola.com.br)