45 – Janeiro de 2003

Perspectiva 2003 para o mercado de segurança da informação

Passados quase doze meses da última previsão para o mercado de segurança da informação no Brasil, nos deparamos com inúmeras surpresas, o que torna ainda mais difícil prever o cenário para o ano de 2003. Contudo, conhecemos novas variáveis que nos ajudam agora a corrigir desvios de entendimento e nos dão subsídios para um prognóstico mais próximo da realidade.

Vimos o mercado, como um todo, reagir com pavor ao evento de 11 de setembro, mas não como todos esperavam. Apesar de criar uma nova percepção de risco da informação para muitas empresas, os investimentos não ocorreram na mesma proporção. Os orçamentos não foram compatíveis com a necessidade de eliminar vulnerabilidades crescentes, reduzir riscos e minimizar os impactos ao negócio. Talvez tenha faltado fôlego financeiro, ou então vontade e instrumentos que melhorassem a estimativa de retorno sobre os investimentos.

É bem verdade que a expectativa política no período eleitoral, as conseqüentes incertezas e o período de transição de poder, transformaram boa parte do ano de 2002 em períodos de cautela, estudo, acompanhamento e conseqüente estagnação de investimentos.

Em contrapartida, vimos a norma de segurança da informação ISO 17799:1 figurar como uma das principais promessas para os próximos anos. O fato de existir um instrumento de orientação executiva como este, propondo uma base comum para a confiança nos relacionamentos corporativos, e principalmente, fornecendo às empresas uma abordagem de gestão de riscos voltada aos interesses e necessidades do negócio, promovem otimismo generalizado no mercado.
Quase duas centenas de empresas ao redor do mundo já estão certificadas pela norma BS7799. Por hora, apenas duas no Brasil, mas o crescimento exponencial do interesse pela conformidade, seja com objetivos de marketing, fortalecimento da imagem ou criticidade do negócio e sua operação, tornam promissor este padrão.

As experiências obtidas durante o ano através de atividades de consultoria, gerência e modelagem de soluções de segurança, palestras e ainda como professor de Gestão de Segurança da Informação nos curso MBA da Fundação Getúlio Vargas – mantendo contato com alunos de perfil gerencial – corroboraram para a consolidação desta perspectiva 2003 para mercado brasileiro de segurança.

- Diagnosticar os riscos de segurança. Este deverá ser o foco de parcela representativa do mercado. Qualquer que seja a decisão - investir, postergar ações, assumir o risco ou definir prioridades de investimento - deverá ser sustentada por análises de segurança abrangentes. Acredita-se que 2003 será o ano das descobertas. O período em que as empresas verão listadas em relatórios de análise, os riscos obtidos pelo levantamento de vulnerabilidades e pontos positivos encontrados, ameaças

potenciais e impactos, considerando as necessidades e estratégicas da empresa. Este instrumento deverá ser usado como bússola de orientação dos investimentos, da priorização de atividades e construção de um Plano Diretor de Segurança mais abrangente.

- Priorizar análises integradas em detrimento de análises isoladas. A segurança da informação deverá estar mais alinhada com os interesses e necessidades do negócio. Por isso, as análises de segurança isoladas, limitadas à investigação em ativos tecnológicos, deverão dar lugar a análises de risco. Serviços capazes de diagnosticar os riscos da empresa através do trinômio: pessoas, processos e tecnologias; buscado identificar o relacionamento com os componentes críticos do negócio. Desta forma, o gestor terá em mãos um instrumento de apoio para dimensionar os investimentos, priorizar atividades e obter o melhor retorno.

- A busca por organizar corporativamente a gestão de segurança da informação deverá continuar. Apesar de não ter sido concretamente definido no organograma de muitas empresas, o Security Office continuará sendo um objetivo perseguido. Desta vez, deverá se buscar argumentos nos resultados da análise de riscos, nos impactos ocorridos no período e nos exercícios de ROI para justificar esta estrutura. A tendência é que se aproximem cada vez mais da estrutura de gestão de qualidade - ligado comumente ao comitê executivo - por conta da similaridade entre o processo e a norma de qualidade, e o modelo de gestão e a norma de segurança ISO17799.

- Retaguarda para garantir a performance e o foco. Por mais este ano, as empresas deverão contar com o apoio – cada vez mais atuante - de empresas especializadas em segurança da informação, como forma de reduzir custos marginais e garantir a performance das atividades e resultados dos projetos. Dificilmente uma empresa que não preste serviços especializados em segurança conseguirá manter uma equipe de profissionais com competências em múltiplas tecnologias e processos, garantindo constante capacitação e certificação, sem onerar suas operações. A tendência é que as empresas mantenham um núcleo com representantes dos departamentos-chave e sob a coordenação de um Security Officer, contando com a consultoria para seu sua retaguarda de segurança.

- Revisão da Política de Segurança. As empresas que possuem uma política de segurança deverão revê-las à luz das recomendações sugeridas pela norma de gestão de Segurança da Informação ISO17799. Aquelas que ainda não desenvolveram diretrizes, normas, procedimentos e instruções deverão fazê-lo em sinergia com os controles propostos pela norma, a fim de estabelecer uma base comum de suporte a novos negócios e a operação da empresa sob risco controlado.

- A certificação ISO17799 ainda não será um objetivo para 2003. Estamos diante de uma norma recém formatada, apesar de ter sido originada da norma britânica BS7799: parte 1. A segunda parte da norma BS - única sujeita à certificação - ainda está sob análise para então produzir sua versão ISO. Enquanto isso, muitas empresas já buscam alinhamento aos exatos 127 controles propostos pela norma e principalmente em se estruturarem para operacionalizar o *framework* de segurança

proposto pela parte certificável: Information Security Management System (ISMS). Este movimento, apesar de tímido, é crescente e motivado pela necessidade de um diferencial competitivo, pela imposição parcial de um parceiro da cadeia produtiva, por impactos financeiros sofridos ou pela preparação intencional de uma futura certificação.

- Ações consistentes focadas no Peopleware. O ativo humano, além de fundamental para a operação das empresas, oferece também um dos maiores índices de risco. Diante dessa percepção, confirmada pelas últimas pesquisas de segurança, as empresas deverão investir maciçamente na conscientização dos funcionários, na capacitação dos operadores de processos críticos e principalmente dos usuários finais que detêm parcela representativa de responsabilidade quando manuseiam, armazenam, transportam e descartam informações sensíveis. Envolvê-los através de campanhas de divulgação da política de segurança e torná-los co-gestores do risco deverá estar entre os objetivos de 2003.

- O prognóstico do ano passado retorna em 2003. Os planos de continuidade de negócio, compostos pelo plano de recuperação de desastres, plano de administração de crises e plano de continuidade operacional, continuarão sendo importantes para processos críticos com baixa tolerância à indisponibilidade. Apesar disso, as ações preventivas de capacitação, auditoria e monitoramento deverão ganhar fatia representativa dos investimentos, reduzindo os custos provocados pelo mau uso dos recursos de rede, queda de performance e maximização dos riscos por descumprimentos à política de segurança.

- Os Internet Data Centers foram a grande zebra do prognóstico de 2002. O setor de telecomunicações não reagiu como os especialistas esperavam. As pressões dos órgãos reguladores que refletiram no segmento de Data Center, a baixa sensibilização do mercado como um todo associada as grandes estruturas de hospedagem tornaram os serviços pesados e caros para os clientes, afugentando-os. Por conta da baixa demanda, muitos deixaram de existir e os poucos que permaneceram de pé ainda estão por agregar segurança aos seus modelos de negócio, para que um dia possam se chamar: Security Internet Data Center.

- Por mais um ano os cartões inteligentes smartcards e certificados digitais estarão ocupando um espaço cada vez maior nas relações eletrônicas. À medida que forem se tornando mais baratos e viáveis financeiramente, vão substituindo os antigos métodos de autenticação: senha, cartão magnético etc. Resta surgir uma *killer application*, ou melhor, uma aplicação que adicione valor e mostre a aplicabilidade e o retorno da adoção do dispositivo, para torná-los de uma vez por todas, atores onipresentes. O mesmo ocorre com os dispositivos de biometria. Apesar de já existirem teclados, mouses e até notebooks com o recurso embutido, eles ainda estão limitados a operações e empresas cuja natureza impõe um altíssimo nível de segurança.

- Planejamento estratégico. Este deverá ser um dos fatores críticos de sucesso para as instituições que possuem ambientes complexos, tecnologias heterogêneas e ainda mantém unidades geograficamente distribuídas. Quanto maior o desafio de segurança considerando os ativos físicos, tecnológicos e humanos, mais abrangente deverá ser o planejamento. É uma tendência que as empresas iniciem a modelagem do Plano Diretor de Segurança – com apoio irrestrito de consultorias que contribuem com uma visão externa - no último trimestre do ano, a fim de gerar estimativas de esforço, investimento e principalmente para garantir o suporte orçamentário para o ano seguinte.

Foram estas as percepções estratégicas que pude extrair até o momento. Desta vez mais conservadoras que as do ano anterior, mas que felizmente revelam o direcionamento do mercado em busca do amadurecimento. Empresas preocupadas em fazer o que é necessário para que seus negócios tornem-se mais ágeis, produtivos, dinâmicos e assim, alcancem melhora nos índices de competitividade. A segurança pela segurança não se justifica. Todas as ações e decisões devem estar alinhadas, em primeiro plano, com as reais necessidades e os planos estratégicos de curto, médio e longo prazos da empresa.

Pelo que se projeta para 2003, veremos mais uma fase de preparação e organização da segurança dentro das empresas. Um período focado no resultado, com ações objetivas, mas começando onde sempre deveria ter começado: a partir de uma análise riscos abrangente e capaz gerar uma visão integrada da situação dos processos, pessoas e tecnologias. Uma visão que orienta as decisões do executivo, pavimenta as ações do gestor e conduz as tarefas dos técnicos.

Marcos Sêmola *é Mestrando em Economia Empresarial, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor de Gestão da Segurança da Informação na FGV – Fundação Getúlio Vargas, Gerente Nacional de Produtos e Consultor de Segurança da Módulo Security Solutions S.A. É autor do livro Gestão da Segurança da Informação – uma visão executiva, Ed.Campus 2002.*
msemola@modulo.com.br