42 – Agosto de 2002

# De que tipo de Análise o CEO precisa?

As empresas estão todas no meio do turbilhão. Informações estratégicas, táticas e operacionais cada dia mais digitalizadas - quando não geradas somente em meio eletrônico - residindo em computadores poderosos que através de uma malha de alta conectividade e alta pulverização, servem aos equipamentos e sistemas satélites o melhor de suas bases de dados e informações de negócio. Parece que já vivemos o futuro desenhado pelos filmes de ficção científica de outrora. Tudo acessível, na palma da mão, ao toque de um botão e até mesmo sem necessitar de toque físico algum, comandado apenas pela voz e...à distância.

A propósito, discutir os efeitos da tecnologia na mudança da distância entre empresas e pessoas poderia ser um bom começo para uma conversa informal, mas temos que nos privar de assuntos paralelos e menos importantes, para nos prendermos ao que realmente faz a diferença. Continuidade do negócio é o foco aqui.
Não importa neste momento se a empresa explora um segmento menos competitivo, se seu porte ainda não oferece riscos aos concorrentes, ou ainda se domina o mercado. O que importa é que todas elas, organizadas e conduzidas por executivos, têm um objetivo coincidente: garantir a continuidade saudável do negócio.

O que parcela representativa das empresas e seus líderes têm feito, entre outras coisas, é aplicar injeções recorrentes de tecnologia, a fim de ganhar velocidade nos processos, maior precisão e qualidade de seus produtos e serviços, aumentar a competitividade e levar seu negócio a atingir um estágio confortável de saúde financeira - onde se lê: Lucro Líquido do Exercício – que aumentem as chances de continuidade da empresa.
Esta é a regra do jogo até agora. E os benefícios são tangíveis e quantificados pelas análise de ROI – Retorno sobre o Investimento. É indiscutível. Contudo, toda essa evolução tecnológica tem algum senão.

Agora todas essas empresas têm substituído com velocidade pilares de sustentação antes estáticos, estáveis e previsíveis, por elementos tecnológicos dinâmicos, que precisam de atualizações constantes e de futuro imprevisível. Têm reduzido seus ativos humanos em função do ganho de produtividade resultante, e também os ativos físicos. Afinal, serviço eletrônico não precisa de prédio de tijolo, portaria e recepcionista. Mas, para muitas, a análise do nível de risco ocasionados pela substituição desses pilares, sinaliza para uma situação de alto risco. Uma situação que afeta e vai justamente de encontro aos interesses de seus executivos: a continuidade saudável do negócio.

Bom, a essa altura tudo que foi dito pode parecer um discurso contrário à tecnologia e à automatização dos processos. Pode insinuar que todas as empresas têm cometido erros e que o melhor caminho é retroceder. Nada disso. Este é o sentido natural das empresas. A busca pela competitividade, produtividade e lucratividade deve estar sendo sempre perseguida, seja lá qual for a injeção de ânimo que tenha de ser aplicada, tecnológica ou não. Mas o que todos os executivos têm de compreender e colocar em sua lista de

prioridades, é que as mudanças contínuas e inevitáveis provocam sempre instabilidade na estrutura corporativa, nos pilares, e as variações precisam ser medidas e acompanhadas para evitar sobressaltos.

Este é o ponto chave! Os riscos associados à segurança da informação afloram a todo instante. Naturalmente mais presentes em empresas com alto nível de automação e informatização, eles permeiam os três grandes pilares: pessoas, processos e tecnologias.
Cada nova mudança estratégica, tática ou operacional, cada admissão e demissão de capital humano, migração de sistemas de computador, substituição de equipamentos e até mesmo mudanças nas variáveis mercadológicas e de política econômica, interferem direta ou indiretamente nos riscos de segurança do negócio.

Os pilares balançam, sofrem rupturas por vezes imperceptíveis, e vão se tornando frágeis com o passar do tempo. Imprudentemente, muitas empresas não tomam conhecimento desses reflexos, desconhecem as causas e os efeitos por estarem desprovidos de instrumentos adequados para medí-los, ou por falta de conscientização e competência nesta área do conhecimento.
Não nos cabe culpá-los pela falta de competência, afinal tendem a se manter focados em seu core business. Em contrapartida, têm de ter a visão de uma águia para perceber, e até mesmo prever, pequenas mudanças na estrutura que implicarão na condução do negócio.

Felizmente muitas empresas estão saindo da inércia e já se mexem. Algumas pró-ativamente, outras ainda reativamente por força de uma ocorrência que gerou impactos operacionais, financeiros ou arranharam a imagem da empresa. É natural. Sem identificar o inimigo, medir o perigo e projetar os impactos, torna-se difícil para qualquer um justificar ações ou investimentos ao acaso. De acordo com a última Pesquisa de Segurança da Informação da Módulo Security Solutions, 85% das empresas que sofreram algum incidente de segurança, ainda não podem quantificar o valor dos prejuízos causados.
Se pudéssemos sinalizar o grau de amadurecimento geral do mercado em relação à cultura de segurança da informação, através da analogia com o processo evolutivo do andar de um bebê, que primeiro engatinha, depois caminha desnorteadamente até atingir o equilíbrio, poderíamos posicioná-lo bem no meio.

Realizar uma análise de segurança já é prioridade para a grande maioria das empresa, o que vem demonstrar a percepção da necessidade de mapear os riscos. Contudo, ainda há um grande “vazio” no entendimento do que é uma análise de riscos de verdade.

Voltando aos pilares de sustentação do negócio, vemos iniciativas de mapeamento de vulnerabilidades concentradas puramente nos ativos tecnológicos, ou seja, instrumentos destinados a analisar e identificar falhas de computadores, redes e sistemas. Evidente que são atividades importantes mas não suficientes para, isoladamente, diagnosticar com precisão os reais riscos que envolvem a operação da empresa. Muitos outros pilares convivem com os pilares tecnológicos e dependendo da natureza do negócio, estes podem ser ainda mais relevantes para a sustentação.

O que venho chamando – há algum tempo - de nova geração de análise de riscos, envolve não só uma mudança na amplitudes horizontal e vertical da análise, bem como o

mapeamento do relacionamento de todos esses ativos - ambientes, equipamentos, sistemas, pessoas, processos e as informações - com os processos de negócio. Parte do segredo de um diagnóstico preciso dos riscos de segurança está na orientação das ações sobre os ativos, feita pelas necessidades do negócio. O negócio é que manda!

Quando um computador que rode a aplicação Internet Banking, por exemplo, têm uma falha que potencializa um incidente de segurança, para executivos, investidores e a comunidade em geral, o que falhou foi o produto ou serviço suportado pela máquina e nada mais. A fração visível, ou a fração prioritária, é justamente o processo de negócio – neste exemplo o Internet Banking - que serve de interface para os clientes, parceiros e demais elementos da cadeia produtiva.

É sensato dizer que esta camada de ativos (lembrando que transcendem os tecnológicos) é indispensável para a operação e será o alvo das ações de segurança, pois contém vulnerabilidades, mas não pode ser confundida com instrumento para a definição de prioridades. Quando isso acontece, vemos ações redundantes sobre os ativos e de retorno discutível, vemos processos de negócio parcialmente atendidos e, consequentemente, o nível de risco projetado, não atingido.

Um bom balanço do que foi falado até agora pode ser resumido pela necessidade que todas as empresas têm de investir gradativamente, de buscar a melhor relação custo vs benefício e direcionar as medidas de segurança para reduzir efetivamente os riscos de acordo com a prioridade de cada componente de negócio.

Decisão. É tudo que os executivos ligados à segurança e Security Officers precisam tomar a todo instante. Que grau de risco estará disposto a assumir. Qual o percentual do investimento de TI deve destinar para a segurança. Quais as ações emergenciais para ameaças iminentes. O que postergar e priorizar já que o montante de investimento é reduzido. Quais os ativos devem ser agrupados em um mesmo projeto para proporcionar maior redução de riscos de uma só vez. Que tipo de ativo oferece maior risco para a continuidade operacional. Como planejar os investimentos em segurança para os próximos anos.
Estas são uma mostra dos dilemas que rodeiam a gestão corporativa de segurança da informação. Perguntas que comumente ficam sem respostas pela ausência de um diagnóstico dos riscos que seja abrangente, preciso e, principalmente, orientado e contextualizado às necessidades do negócio.

***Marcos Sêmola*** *é Mestrando em Economia Empresarial, MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Professor da cadeira de Segurança da Informação da FGV – Fundação Getúlio Vargas, Gerente Nacional de Produto e Consultor de Segurança da Módulo Security Solutions S.A.*
*msemola@modulo.com.br*