24 – Outubro de 2000

No limite da insegurança.

Informações da Febraban revelam que em 1999 no Brasil, 9,3 trilhões de operações foram realizadas sem a intervenção de funcionários, representando 67% do total de transações. 2,6 bilhões de cheques compensados, contra 4,6 bilhões de transações eletrônicas. De 98 para 99, o número de transações pela Internet saltou de 38,7 milhões para 126,3 milhões.

Todos os segmentos de mercado estão vivendo o mesmo momento. Integrando doses cada vez maiores de tecnologia aos seus negócios, otimizando seus ambientes, personalizando e automatizando seus produtos e serviços. Cada vez mais conectados – principalmente através da Internet - para compartilhar informações pensando em explorar as maravilhas prometidas pela informática.

Contudo, pressionados pela competitividade do mercado – onde qualquer informação estratégica pode representar o diferencial que a colocará na liderança – são motivados a implementar novas idéias e aplicações sem se preocupar com todos os elementos que garantirão seu sucesso.

É a miopia do mercado e de seus executivos, ou visão do iceberg (expressão adotada principalmente por que a parte de gelo submersa representa aproximadamente 7 vezes mais do que a fração de gelo visível).
Esta visão limitada os faz perceber apenas algumas variáveis que formam a "equação da segurança", ou melhor, a porção do iceberg que está sobre a linha d'água - problemas de segurança isolados e principalmente tecnológicos – enquanto há muitos outros problemas igualmente importantes como os de infra-estrutura física, do ambiente tecnológico com seus dispositivos e sistemas, das aplicação, da própria informação e das pessoas.

Correio eletrônico, EDI – Eletronic Data Interchange, ASP – Application Service Provider, Enterprise Resource Planning, Celular WAP, Intranet, Extranet, Acesso Remoto via Notebook... uma gama de tecnologias para gestão, automação, conectividade e compartilhamento de informações que estão fazendo parte do ambiente corporativo, mas que podem, ao invés de só agregar valor ao negócio, representar grandes vulnerabilidades, riscos e ainda potencializar impactos ao negócio que coloquem em dúvida sua própria continuidade.

De acordo com órgão de pesquisa WorldTalk, 31% dos emails corporativos são lixo ou representam algum perigo: 10% SPAM, 9% vazamento de dados confidenciais, 4% mensagens com anexos gigantescos ou mensagens não-spam enviadas para centenas de pessoas, 4% pornografia, ofensas religiosas, éticas ou morais, 2% piadas e 2% contaminadas por vírus e bombas de email.

As empresas estão vivendo NO LIMITE!
Integram todos os elementos da cadeia produtiva – fornecedores, parceiros, distribuidores e o governo - através de conexões híbridas, e ainda compartilham remotamente informações

estratégicas com os funcionários, que com seus notebooks acessam a rede corporativa. Tudo isso – que aparentemente só agregaria valor e se converteria em benefícios – comumente não está amparado por um planejamento corporativo de segurança da informações, capaz de minimizar os riscos de vazamentos, invasões, roubos, acessos indevidos, retrabalho, perda de produtividade, perdas financeiras e ainda prejuízos à imagem.

Segurança da Informação é o fator crítico de sucesso, elemento que viabiliza aplicações, e fundamental para garantir a integridade, confidencialidade e disponibilidade, quando se manuseia, armazena, transporta e descarta informações. Reduzir os riscos, minimizar os impactos no negócio e preservar os investimentos são benefícios diretamente associados à uma Solução Corporativa de Segurança da Informação.

Para que se alcance esse estágio, é preciso estar sensibilizado e conscientizado para que se inicie um planejamento estratégico (orçamento e plano de ação) capaz de orientar toda a empresa quanto às melhores práticas no relacionamento com a informação.

Pode parecer que os executivos têm dificuldade em perceber o retorno sobre o investimento em segurança, mas contrariando esta afirmação, eles já possuem todos os argumentos que os levem a obter sucesso nessa iniciativa. Além dos números expressivos resultantes de uma análise de ROI (quando se mensuram as perdas diretas e indiretas por falta de segurança), eles mesmos já possuem modelos mentais exercitados outrora, quando se mobilizaram para analisar e resolver os problemas associados ao Bug do ano 2000, à implantação dos sistemas de gestão ERP – Enterprise Resource Planning e ainda quando se mobilizaram para adquirir a certificação ISO.

Vamos entender... em tempo de resolver o problema dos sistemas para a virada do ano 2000, concluíram que se tratava de um problema generalizado, necessitava de uma ação corporativa e que precisavam estar *compliant* com o bug. No momento de otimizar seu modelo de gestão com as soluções ERP, concluíram com a análise que para obter sucesso, necessitavam ter uma visão estratégica, mudar e adaptar os processos e ainda manter o controle centralizado. Já na iniciativa de certificação de qualidade ISO, perceberam e dependência da conscientização da alta administração, a criação de normas e procedimentos, a certificação, implantação e a administração constante.
Todos esses aspectos observados nos momentos já vividos pelos executivos e empresas, são igualmente importantes para se conseguir modelar uma solução de segurança corporativa. Portanto, já possuem o "caminho das pedras" para se atingir o nível de segurança adequado para a natureza do seu negócio.

É importante entender que não há solução de segurança padrão capaz de resolver e servir à todas as empresas. Uma análise detalhada do negócio – identificando o relacionamento da empresa com a informação, perímetros, dependências, tolerâncias e conexões com os elementos da cadeia produtiva – associada a um planejamento corporativo, são essenciais para modelar uma solução que irá proteger as informações que sustentam o seu negócio.

A experiência herdada e acumulada durante anos nos diversos projetos de tecnologia e segurança da informação, me permite arriscar números que representem o percentual que

deve ser dedicado à segurança da informação. Se sua empresa é tradicional e adota a tecnologia com entusiasmo (se é que ainda existem empresas vivas que não o fazem), já com o pé na nova economia, pense em definir um orçamento para segurança de até 20% do que você investirá em TI – Tecnologia da Informação. Mas se seu negócio é exclusivamente da nova economia, comece a pensar em investir em segurança até 50% do que investirá em TI. Estes percentuais de investimento são a fronteira entre continuar crescendo ou estar fadado à regressão e possivelmente à descontinuidade.

Diante disso, avalie os riscos que está assumindo, os impactos a que está suscetível e deixe de operar no limite! Segurança da Informação é reduzir os riscos, minimizar os impactos, maximizar os investimentos e fundamentalmente apoiar a continuidade competitiva do seu negócio.

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