40 – Maio de 2002

Os sete ações de empresas muito eficazes em Segurança da Informação

Muitos livros, dos quais grande parte *bestsellers*, adotam títulos similares a esse para realçar o comportamento, as técnicas e ferramentas que vêm mostrando eficácia em cada um dos ramos do conhecimento e da gestão. Seguindo esta idéia aparentemente campeã, me perguntei: por que não realçar também os pontos positivos que têm trazido bons e reais resultados às empresas por conta de ações ligadas à gestão da segurança da informação!?

Ao exercitar a resposta, confirmei a necessidade que temos de obter conhecimento organizado e preferencialmente voltado à aplicação imediata que gere resultados no menor prazo possível. Não poderia ser diferente para os aspectos tecnológicos e os ligados à proteção da informação que sustentam os negócios.

Por estarmos falando apenas de sete ações mais eficazes, serão apresentadas apenas diretrizes corporativas, como se tivéssemos manuseando uma grande bússola que apontasse a direção. Felizmente, um instrumento de orientação já adotado por algumas empresas, concentradas principalmente no segmento financeiro, talvez pela própria natureza de sua atividade. Vejamos os resultados...

1. “Aculturação” corporativa

Como sabemos, toda e qualquer empresa - para alcançar um nível de administração de riscospara proteger suas informações e, conseqüentemente, garantir a continuidade operacional do negócio - , depende da saúde dos seus ativos físicos, tecnológicos e humanos.

É fácil compreender a importância que a sala de hospedagem dos equipamentos tem para o funcionamento da empresa, bem como a importância dos sistemas computadorizados, redes e bancos de dados, mas os fatos têm revelado – infelizmente por fatos de quebra de segurança – o ativo humano como um dos mais críticos. Estes resultados são coerentes, afinal os seres humanos cometem erros, têm personalidade ímpar, características dinâmicas de relacionamento interpessoal e, principalmente, não vêm com manual de operações.

Por conta disso, apresentam comportamentos dos mais diversos e imprevisíveis, pondo em risco – de forma intencional ou não – a confidencialidade, integridade e disponibilidade das informações a que tem acesso. Desta forma, as empresas eficazes criam processos contínuos e flexíveis para “aculturação” dos funcionários, lançando mão de treinamentos formais, seminários e palestra informais, culminando com a adoção de material de comunicação endomarketing como folhetos, mouse pads, broches, e até mesmo protetores para a tela de seus computadores a fim de formar um movimento cultural de dentro para fora.

Os resultados são excepcionais. Cada um sente-se parte de um movimento de auto-proteção e de preservação da empresa onde trabalha. Estes reflexos atingem o ponto alto quando o próprio mercado percebe a preocupação de todos os integrantes da organização com a segurança.

2. Security Office

Por considerar acertadamente a segurança e seus aspectos como um problema generalizadamente corporativo e associado aos diversos ativos, distribuídos física e logicamente, e ligado diretamente à natureza e estratégia do negócio, muitas empresas já estão administrando o assunto através do conceito de governança corporativa.

Desta forma, criam comitês executivos de segurança comumente coordenados por um Security Officer capaz de organizar as demandas e planejar, eu disse planejar, as ações de curto, médio e longo prazos. Evidentemente, este movimento precisa de autonomia e total sintonia com os valores e diretrizes da empresa. Desta forma, este hábito eficaz vem acompanhado da especificação de um plano orçamentário próprio para promover a gestão da segurança dentro de um processo corporativo vivo.

3. Outsourcing especializado

Por que realizar altos e contínuos investimentos em infra-estrutura complexa, recursos físicos, tecnológicos e humanos profunda e diretamente ligados à segurança da informação – como exige a atividade – já que este não é o *corebusiness* da minha empresa?

Depois de responder a esta pergunta, muitas companhias terceirizaram parte das atividades e dos recursos que não trazem retorno vinculado diretamente aos seus produtos e serviços. É relativamente simples perceber os desvios de foco. Você vê sentido em contratar e manter uma equipe certificada nacional e internacionalmente, quase sempre muito onerosa, e necessariamente multi-especializada em diversas tecnologias sensíveis, - como sistemas operacionais, servidores, firewall, roteador e bancos de dados - , se ela for subutilizada, ou seja, se as remunera por 365 dias/ano e só usufrui de seu potencial por uma fração desse tempo!?

Com o questionamento, a grande maioria das empresas – excetuando aquelas que mantêm atividades de natureza intrinsecamente críticas e que, por isso, precisam avaliar melhor esta postura – aderem ao movimento de terceirizar parte das atividades de segurança com empresas especializadas. Estas, além do expertise específico e continuamente atualizado, passam a atuar como retaguarda de segurança, responsável, na maioria dos casos, por atividades de consultoria e implementação técnica que demandariam das empresas grande mobilização de recursos.

Este hábito têm mostrado-se eficaz por, entre outras coisas, servir de instrumento para o Security Officer e os Comitês Executivos, que continuam gerindo corporativamente os ativos e coordenando todas a ações de segurança próprias e de terceiros.

4. Plano Diretor de Segurança

Tem-se a "aculturação", os gestores e o apoio externo para consultoria e implementações técnicas, mas ainda é necessário desenvolver um plano de ação de segurança da informação específico para empresa que contemple atividades de curto, médio e longo prazos.

Estamos falando do Plano Diretor de Segurança da Informação, que deve ter escopo corporativo máximo e contar mais uma vez com o apoio externo a fim de adicionar valor a partir de uma visão externa, comumente isenta e não viciada.

As atividades ligadas ao desenvolvimento do plano devem ser orientadas por uma metodologia de mensuração do grau de importância dos processos de negócio, a sensibilidade de cada um deles associado aos conceitos de segurança: confidencialidade, integridade, disponibilidade, e dos aspectos autenticidade e legalidade. O passo seguinte será mapear os ativos físicos, tecnológicos e humanos que mantêm o negócio funcionando. Depois deste complexo diagnóstico, o mapeamento da situação atual deve ser cruzado com os planos estratégicos da empresa para que então seja gerido um planejamento plurianual de segurança da informação que apontará o caminho para o Security Officer.

A inexistência deste instrumento ou a sua má qualidade podem representar a perda de foco, o baixo retorno sobre os investimentos e, possivelmente, a inconsistência das ações. Sentido contrário ao perseguido pelas empresas que acertadamente já adotam esta ação em busca de sinergia e integração das atividades que irão reduzir efetivamente dos riscos.

5. Desmembramento do plano de ação

Gerir a segurança e todos seus elementos é uma tarefa complexa e proporcional ao porte do seu negócio e diretamente ligada à natureza de sua atividade. Sabe-se que cada negócio irá requerer um nível próprio de administração de riscos , adotando controles específicos e capazes de conduzí-lo aos parâmetros especificados por seus gestores. Por conta disso, desmembrar o desafio tem sido um hábito eficaz para muitos, principalmente se considerarmos os obstáculos orçamentários e a incapacidade de tratar todos os males ao mesmo tempo e com o mesmo esforço. Desta forma, de posse do plano diretor de segurança da informação, que propõe ações corporativas integradas, subdivide-se a empresa de acordo com o grau de criticidade de cada parte, priorizando ações mais relevantes e que possam estar cobertas pelo orçamento aprovado.

É evidente que a melhor situação seria tratar todos os elementos simultaneamente e implementar o plano na íntegra mas, na prática, existem limitações, e quase sempre a necessidade de justificar matematicamente e financeiramente os investimentos.

Assim, o hábito saudável e eficaz está, por exemplo, na elaboração gradativa de uma Política de Segurança consistente e personalizada que aos poucos vai subsidiando ações de diagnóstico, especificação, implementação e administração sem perder a integração e sinergia sugeridas pelo Plano Diretor de Segurança da Informação.

6. Conformidade com as normas BS7799/ISO17799

Talvez antecipar o futuro e buscar conformidade com normas internacionais de segurança da informação possa parecer que não signifique muito neste momento, mas certamente irá proporcionar um grande diferencial competitivo em curto prazo, e talvez será elemento fundamental e impeditivo para as relações comerciais se pensarmos em prazos maiores.

A norma britânica BS7799:1 e a sua equivalente americana ISO/IEC 17799, que definem um código de conduta para a gestão de segurança da informação, têm sido estudadas pelo Security Officer e pelo comitê executivo, a fim de adequar os processos de segurança para viabilizar a candidatura da empresa à certificação. Felizmente, a busca pela conformidade já é praticada por algumas empresas pioneiras. Além de oferecer um veloz amadurecimento das equipes e dos gestores envolvidos em seu estudo, a norma orienta as empresas na direção certa, colocando-as na trilha da conformidade.

7. Questionamento e busca constantes

Acomode-se e acumulará riscos. Pode parecer exagerada, mas a afirmativa é pertinente, afinal, sempre que houver uma mudança que implique no ambiente corporativo, seja externa - de caráter mercadológico, financeiro e político-, ou interna - de caráter físico, tecnológico e humano - , novas falhas de segurança surgirão e, portanto, novos riscos somarão aos existentes.

Diante disso, adotar uma postura corporativa de constante questionamento, que induz a novos diagnósticos, novas implementações e busca de novos controles que conduzam o nível de risco ao patamar especificado para o seu negócio, completa nossa lista.

A segurança da informação deve ser tratada como um processo contínuo, flexível e dinâmico, pois só assim sua empresa poderá estar preparada para superar os desafios que estão por vir. Faça como as companhias mais eficazes em segurança da informação. Reúna os executivos e responsáveis diretos. Promova projeções e análises de situações de curto, médio e longo prazos. Dimensione os orçamentos. Mensure os resultados do investimento. Envolva todos os funcionários. Fomente o acompanhamento de índices e indicadores. Planeje ações integradas e, principalmente, não deixe seu processo de gestão estagnar.

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 Nacional de Produto e Consultor de Segurança da Módulo Security Solutions S.A.*
msemola@modulo.com.br