47 – Maio de 2003

Quebra-cabeças da Gestão da Segurança

Porque se ouve tanto falar de Gestão de Segurança? Será pelo excesso de atividades e projetos, pelo volume de correções que os computadores e sistemas vêm sofrendo mês a mês, ou pelo aumento da maturidade do mercado a partir da formação de equipes internas e normas específicas de segurança da informação? A resposta pode estar na mistura de tudo isso. Em outras áreas do conhecimento, na década passada, vimos as consultorias fortalecidas pela complexidade dos projetos de qualidade, reengenharia, bug do milênio e todos os demais projetos de inovação tecnológica. Eram grandes projetos que geravam demanda natural para empresas dispostas a compreender o problema e desenvolver uma solução específica para o cliente.

No mercado brasileiro, as empresas ainda se encontram em estágios de maturidade de segurança distintos. Muitas ainda se preocupam em solucionar problemas pontuais que aparecem esporadicamente. Outras já se planejam antecipadamente para garantir a operação de um novo negócio ou atividade sob risco controlado. Um número quantitativamente representativo, nem sequer percebe o risco e se mantêm inerte, assumindo os riscos às escuras e administrando os prejuízos financeiros e impactos do dia-a-dia como fatos rotineiros e inerentes à sua atividade. Em contrapartida, alguns segmentos e empresas já estão em estágio mais maduro. Aprenderam com a vivência das fases anteriores – por onde quase todas passam – e já vivem uma nova realidade.

Para este grupo ainda seleto, segurança da informação se faz de forma integrada, unindo as ações voltadas para os ativos tecnológicos, bem como para os ativos físicos e principalmente humanos. São empresas que buscam a competitividade, agilidade e, assim, recorrem ao mercado em busca de ajuda objetiva. Mantêm-se focadas em suas atividades fim sem, no entanto, perder o controle sobre seus bens mais valiosos. O reflexo disso é a formação de pequenas equipes técnicas internas, montadas para a condução e coordenação de projetos de segurança, muitas vezes executados com recursos terceirizados ou por empresas especialistas contratadas. Elas têm em mente a necessidade de proteger sua imagem, garantir a lucratividade e investir em segurança continuamente. A obtenção de uma visão integrada dos riscos possibilitou-os compreender a necessidade de processos de gestão. Rotinas, padrões e estruturas posicionadas no organograma da empresa, que possam manter viva e funcionando a "máquina" de administração de controles e riscos, respondendo com velocidade e objetividade às mudanças previsíveis que as variáveis internas ou externas apresentarão. Um framework de segurança alinhado, em primeiro lugar, aos interesses estratégicos da empresa, às características específicas da sua atividade e, porque não, ao código de prática proposto pela norma internacional BS7799.

Chegamos ao ponto chave. Este estágio de maturidade fez com que as empresas desse grupo ainda seleto, pensassem mais friamente no retorno que os investimentos em segurança precisam dar. Tem que haver objetividade e, simultaneamente, têm que fugir da simples aparência de segurança ou a falsa sensação de conforto operacional. Além disso, é preciso compreender que as ameaças e todos os seus agentes também vivem estágios

embrionários e começam a se desenvolver e aprimorar. Seu concorrente ou funcionário insatisfeito não são mais os mesmos e podem lançar mão de artifícios mais modernos e proporcionalmente mais destrutivos para o seu negócio.
Este cenário, que não é novo para muitos, requer uma estrutura auto-sustentável operacionalmente: um Security Office e a figura de um profissional CSO – Chief Security Officer. Precisa de uma equipe mínima – para que não onere sua operação ao desfocar de seu *corebusiness* - que possa organizar e manter as atividades e ações que forem terceirizadas junto às consultorias especializadas, dentro do trilho estratégico da empresa. O que vemos com este movimento é a materialização de um Modelo de Gestão de Segurança da Informação. O recheio para o framework ISMS – Information Security Management System citado e descrito pela norma BS7799.

Arrisco um passo-a-passo prático para que este objetivo torne-se menos distante:

- Promova a conscientização da importância da informação para a empresa em todos os seus níveis hierárquicos;
  - Realize seminários e palestras;
  - Compartilhe literatura especializada que associe tecnologia e negócio;
  - Desenvolva uma campanha de sensibilização;

- Destaque uma pequena equipe, pré-disposta e interessada em segurança da informação;
  - Capacite um ou mais funcionários em cursos de segurança especializados;
  - Garanta a certificação técnica nas tecnologias mais sensíveis ao seu negócio;
  - Nomeie um responsável pelo embrião da estrutura de gestão de segurança;

- Execute uma Análise de Riscos integrada, capaz de demonstrar com dados reais, as ameaças, os riscos e impactos à que a empresa está sujeita, considerando os ativos físicos, tecnológicos, humanos e associando-os às características do negócio;
  - Terceirize o serviço de Análise de Riscos ou;
  - Capacite uma equipe técnica específica munida de ferramentas especializadas para orientar as atividades de Análise de Riscos;

- De posse dos resultados da análise, promova nova conscientização, mas desta vez só do corpo executivo, a fim de viabilizar a nova estrutura Security Office no organograma, seguida da encomenda de um Plano Diretor de Segurança que irá ajudá-los no futuro dimensionamento orçamentário.
  - Seja objetivo e fale a linguagem do negócio: lucro, prejuízo e retorno sobre o investimento;
  - Mostre a sinergia das ações propostas com a norma BS7799/ISO17799, revelando a importância do código de prática, do framework ISMS e da possibilidade futura de certificação como diferencial competitivo;
  - Demonstre a possibilidade de utilizar a norma, no primeiro momento, como instrumento de orientação de padrões e práticas adotadas mundialmente por empresas de diversos segmentos;

  - Sinalize a possibilidade de atingir com o amadurecimento do modelo de gestão, a certificação de segurança BS7799 em perímetros específicos, não necessitando envolver toda a empresa e seus processos de uma só vez;

- Não abra mão de ajuda externa especializada, mesmo que agindo somente como retaguarda técnica ou estratégica de segurança, pois além de somar uma visão isenta e descontaminada dos processos e métodos conhecidos da empresa, certamente irá adicionar ricas experiências e competências ímpares que só uma empresa especializada em consultoria e gestão integrada de segurança da informação poderia compartilhar.
  - Identifique seu parceiro ideal pela competência estampada no sucesso de seus projetos e no tempo de experiência;
  - Identifique seu parceiro ideal pela competência técnica presente nos profissionais de seu quadro funcional;
  - Identifique seu parceiro ideal pela qualidade de sua metodologia de trabalho e sinergia com a norma BS7799/ISO17799;
  - Identifique seu parceiro ideal pelo posicionamento como retaguarda de segurança, tornando-se um aliado à sua equipe interna e ao mesmo tempo complementar técnica e estrategicamente nas ações complexas;

- Se a empresa já estiver pensando em certificação, conformidade com a norma etc, é bom se organizar *top-down* e tratar o assunto no mínimo com a mesma seriedade com que a busca pela certificação de Qualidade ISO9000 fora tratada. Aliás, os temas têm muito em comum, afinal, ambas adotam o modelo PDCA (Plan, Do, Check e Act) como estrutura básica de funcionamento da estrutura de gestão, registro e controle.

  - Mais uma vez a ajuda externa pode se tornar necessária - mesmo que em apenas alguns momentos do projeto - e, para isso, você deve identificar seu parceiro ideal pela experiência, domínio da norma e, preferencialmente, pela própria experiência de ter se certificado.

É bom parar por aqui, caso contrário o artigo passa a livro. Ah! E por falar em livro, peço licença aos leitores para anunciar o lançamento do meu primeiro livro: Gestão da Segurança da Informação – uma visão executiva, Ed.Campus 2003. Toda a linha de raciocínio desenvolvida e compartilhada homeopaticamente nos artigos, acabaram confinadas em uma publicação voltada ao profissional que custodia informações, lida com ameaças e precisa obter uma visão integrada dos riscos para ajudar a sua empresa. É resultado legítimo da estrutura e legado compartilhados pela Módulo no exercício da profissão como Consultor de Segurança, das pesquisas paralelas, contato com clientes, além das experiências interativas como docente da cadeira de Gestão de Segurança da Informação nos cursos MBA da FGV – Fundação Getúlio Vargas.

Mais uma vez desculpo-me pela informação de interesse duvidoso e, pretensiosamente me auto redimo na esperança de estar contribuindo com a comunidade de segurança, com os profissionais que já trabalham no setor ou mantêm planos, e ainda com cada uma das pessoas que trabalham nos setores público e privado e que, de alguma forma, tem um

importante papel – mesmo que limitado a uma única "engrenagem" da grande "máquina" de negócio - na formação da cultura de segurança no Brasil.

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 Project Manager da Schlumberger Worldwide IT Partner..*
marcos@semola.com.br