50 – Agosto de 2003

Preciso justificar os investimentos, mas como?

Você já deve ser feito esta pergunta ao menos uma dezena de vezes, assim como eu. Mas não espere encontrar aqui uma fórmula mágica ou uma receita infalível para respondê-la e aprovar todos os seus projetos de segurança da informação. É verdade que procuramos por isso há tempos, mas simplesmente ainda não existe ou não foi inventado um método aplicável a qualquer situação. O que sabemos é que existem valores corporativos básicos e modelos de apoio à tomadas de decisão.
Em geral, o executivo de média e alta gerência, responsável por aprovação de investimentos representativos, adota em primeiro nível um modelo de avaliação de oportunidades simples. Se o retorno financeiro ou redução dos custos proporcionados pelo projeto for maior do que o montante de seu investimento, a iniciativa tem o potencial de ganhar importância e consequente aprovação. Simples não?
Sim, se todos os projetos e seus resultados pudessem ser facilmente quantificados financeiramente. Esse é o desafio.
As atividades que podem compor um projeto de segurança da informação são muito heterogêneas, tratando de aspectos físicos, tecnológicos e humanos. Podem assumir um posicionamento reativo, normalmente mais fácil de se justificar pois já existem evidências do problema, ou um posicionamento pró-ativo se antecipando ao suposto problema e por isso, bem mais difícil de se equacionar. Diante de tantas dificuldades para justificar os investimentos, temos que nos prender aos números. Tentar à todo custo transformar campanhas de conscientização, tunning de sistemas operacionais, segurança em aplicações, dispositivos de autenticação, criptografia, normas, padrões, treinamentos, firewall, controles de acesso físico e até consultoria, em unidades de medida válidas para o julgamento do aprovador.

Não podemos ignorar outros valores, que não apenas o financeiro, capazes de apoiar a justificativa de investimentos. Eles tendem a variar de empresa para empresa, escopo para escopo e até mesmo de projeto para projeto. A estratégica de ser uma empresa pioneira pode estar à frente do simples motivo de ROI direto, ou seja, o aprovador pode decidir pelo investimento em busca do fortalecimento e valorização da marca e não simplesmente pela redução de custo direto que o projeto pode trazer. A empresa pode ainda estar interessada na corformidade com leis e padrões, em certificações internacionais, em uma grande campanha de marketing ou na legítima vontade de estar preparada para suportar projetos futuros.

De qualquer forma, independente dos valores considerados por um determinado aprovador em um determinado momento da empresa, o apelo financeiro sempre tem respeito e acaba pesando em qualquer decisão. Para isso, temos que fazer o “dever de casa”.
Comece definindo índices e indicadores de performance que possam servir de base para a coleta de evidências ao longo do tempo, seja prejuízo financeiro direto ou outras situações que acabam por gerar os mesmos prejuízos como: perda de rendimento, perda de clientes, ações trabalhistas, multas, aumento de custos operacionais, tempo de paralização da

produção, indisponibilidade de um sistema crítico, desvalorização das ações, desgaste da imagem, retrabalho, fraudes, sabotagens, erros, impactos ambientais etc.
Estruture um processo de acompanhamento e alimentação dos indicadores e deixe que trabalhem por você. Dê tempo para que acumulem um volume representativo de evidências, tente – pois não é tarefa fácil - convertê-las em números financeiros e extraia dados estatísticos baseados no tempo. Então estude seu projeto e procure mapear a interferência que terá nos processos que são considerados para a alimentação dos indicadores. Essa relação cruzada é fator crítico de sucesso e nos dará uma visão dos benefícios do projeto, medido pela interferência potencialmente positiva nos indicadores. Se com isso pudermos quantificá-la, teremos o ROI financeiro do projeto e estaremos praticamente prontos para justificá-lo.
Contudo, antes de agendar a apresentação do projeto, é preciso fazer um "teste de sanidade", estudando a relação entre o montante financeiro do investimento e o montante financeiro que representa os benefícios do projeto, além do espaço de tempo entre o desembolso para execução e o retorno do investimento.

Sempre que escrevo sobre um assunto que não pode ser tratado como uma ciência exata e envolve variáveis que fogem ao controle, tenho receio de ficar na camada acadêmica sem propor ações aplicáveis ao mundo real. Por isso, proponho uma simulação de cenário como exercício.
Imaginemos uma empresa que há muito vem observando baixa de faturamento e perda de produtividade dos funcionários nas atividades de confecção e entrega dos produtos e serviços aos clientes internos e externos. Diante disso, poderíamos definir índices de acompanhamento para medir a produção por funcionário (controle de entrega), a evolução do faturamento da empresa (balanço por período), o tempo de dedicação à atividade fim (timesheet e log de uso de recursos de rede), o nível de motivação e comprometimento dos recursos humanos (pesquisa de satisfação). Em seguida, precisaríamos definir pequenos processos de alimentação desses indicadores por um período de tempo representativo, seis meses por exemplo. De posse das informações de evolução e medição dos indicadores, teríamos que associar os problemas percebidos com a perda financeira, por exemplo, extrair a relação entre a hora de trabalho e o faturamento produzido.
Agora resta analisar o projeto e seus benefícios para projetar os reflexos positivos nos indicadores. Imaginemos que o projeto possui as seguintes atividades: campanha de conscientização dos usuários, reformulação da política de acesso à Internet, norma de resposabilização pela proteção das informações críticas, implementação de software de crítica e filtragem de acesso aos serviços web e gerenciamento de mudanças. Poderíamos dizer por projeção e associação com os índices de acesso a serviços web desvinculados às atividades da empresa, que por hora um funcionário tem consumido 1/4 em atividades improdutivas representando um montante financeiro (obtido com o RH). A partir daí, com os beneficios do projeto se poderia projetar a redução de uso indevido e assim quantificar financeiramente seu retorno.

Como mencionei inicialmente, fazer com que a empresa tire dinheiro dos cofres de forma autônoma e justificável não é tarefa fácil. Se assim fosse, não precisaríamos exercitar novos modelos, aprender com os erros e acertos e muito menos estaríamos investindo nosso tempo em escrever e ler artigos como estes. Espero ter ajudado. ☺

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