

21 – Julho de 2000

Você acredita no ROI - Retorno sobre o Investimento? Pois deveria.

ROI ou Retorno sobre o Investimento é uma ferramenta antiga e velha conhecida dos empreendedores, investidores e executivos atentos ao mercado e às oportunidades. Construída através do cruzamento de dados reais relacionados a custos diretos, custos indiretos e custos intangíveis, com a projeção de investimentos, obtêm-se um ótimo instrumento para nortear as ações desses executivos.

Parece, em um primeiro momento, instrumento essencial para apoiar uma tomada de decisão, e realmente o é. Analisando-o consegue-se muitas vezes, justificar altos investimentos, mudanças de rumo e estratégia, afinal, torna-se possível projetar o retorno do investimento.

Não existe um único modelo de ROI, nem tão pouco um modelo certo ou errado. O que existe, são abordagens diferentes e visões diferentes do mesmo objeto. A profundidade da análise interfere diretamente neste modelo, agregando um número ainda maior de variáveis e refinamentos. Contudo, todas buscam um resposta mágica para a pergunta: devo realizar este investimento?

Pode soar estranho para muitos, mas a mesma pergunta se aplica também à investimentos na área tecnológica, você sabia? Foi-se a época em que investimentos desse gênero eram vistos com um “mal necessário”. Époça em que se realizavam grandes aquisições – de última tecnologia – e não se preocupavam em medir resultados, projetar o tempo de colher os louros do investimento. Époça em que tais despesas (pois assim é que eram vistos os investimentos), seriam repassadas através do produto ou serviço ao consumidor final ou diluídas em aventuras na ciranda financeira.

Chegou a hora de planejar, projetar, medir e cobrar os resultados da integração entre tecnologia e negócio. Mas também é hora de exercitar mais o ROI em subcategorias, com maior detalhamento. Não basta modelar um macro ROI tecnológico, é preciso abordar tecnologias e problemas mais específicos como a segurança da informação.

O gargalo desse trabalho é notoriamente entender, conhecer e mapear os problemas corporativos, pois sem essas informações, não seria possível desenvolver uma ferramenta de ROI coerente, confiável e pronta para apoiar a priorização das ações e as tomadas de decisão.

O ROI da segurança tem especialmente muitas respostas elucidativas que nos ajudam a reverter a velha imagem de despesa, convertendo-a em investimento e – diga-se de passagem – um ótimo investimento!

Vamos exercitar tratando primeiro os custos diretos... Se cruzarmos o número de contaminações por vírus de computador em um ano, o percentual de funcionários atingidos,

o tempo perdido com a paralisação e o custo homem/hora, perceberemos com nitidez o impacto direto no negócio.

Ao analisarmos o tempo de trabalho consumido pelos funcionários com acesso livre à Internet, acessando informação que nada têm de associação com a atividade profissional e novamente com o custo homem/hora, podemos projetar o impacto na produtividade dos recursos humanos.

Se ainda por ocasião de um desastre, houver a indisponibilidade de um serviço – por exemplo de Internet Banking – multiplique o número de correntistas que o acessam por hora, a economia que a empresa tem por seus correntistas evitarem as agências e migrarem para a Internet e, assim, terá o impacto direto.

Falando agora de impactos indiretos, usando as mesmas situações, podemos realçar os custos relacionados à mobilização de equipes para remover os vírus que infectaram os computadores da rede, o tempo necessário para reconstruir arquivos e informações que se perderam com a contaminação, e ainda possíveis restaurações de cópias de segurança (se existirem). Seguindo os exemplos anteriores, o acesso indiscriminado e sem controle à Internet, pode provocar uma sobrecarga da banda de rede, antecipando investimentos e causando indisponibilidade. Além disso, pode permitir a contaminação por vírus de toda a rede com a execução de programas copiados (download) da Internet e pior, expor a empresa à sanções legais relacionadas à pirataria de software, pedofilia e crimes virtuais.

E os problemas não param por aí, a indisponibilidade dos serviços pode atingir profundamente você e o seu cliente. Primeiro você pelo fato do cliente não ter conseguido realizar uma transação financeira, um investimento ou uma solicitação de cartão de crédito etc. Agora o cliente, que deverá ser reparado através de uma ligação do telemarketing, de campanhas de marketing direto etc.

Agora vem o pior. Custos intangíveis e incalculáveis que põem verdadeiramente em risco a continuidade do negócio. O impacto de uma invasão, seja interna ou externa, causando o roubo de informações, não é fácil de ser calculado. Muitas vezes não se sabe que fim levou aquela informação e muito menos como ela será explorada. Será que estará na mão de um concorrente? Ou ainda na mão da imprensa pronta para um furo de reportagem?

Trata-se de um problema sem dimensão definida. O impacto à imagem é coisa séria e custosa para ser revertida. Gasta-se muito mais recurso tentando reconstruir uma imagem sólida, segura, eficiente e compromissada com o cliente, do que o recurso que foi gasto para construí-la.

Ah! Ainda temos que pensar nos novos negócios que estão por vir e que dependerão da segurança para sua viabilidade. Afinal, que empresa não gostaria de ser o empreendimento que faz acontecer, ao invés de apenas ver o que acontece?!

Bom, de uma maneira geral, projetos de segurança da informação visam proteger a integridade, confidencialidade e disponibilidade das informações, e traz como benefícios: viabilizar e agregar valor aos negócios e aplicações; aumentar o *market-share*; manter a vantagem e o diferencial competitivo; garantir a satisfação dos clientes; elevar a

produtividade dos usuários; reduzir os riscos provocados pelas ameaças; gerar receita e/ou reduzir custos e perdas, e manter a imagem e a liderança competitiva da empresa.

O estudo de ROI definitivamente já faz parte do dia-a-dia dos executivos de tecnologia, e a segurança da informação em especial, já é pauta certa de reunião e motivo de sobra para ser considerada um investimento. Investimento importante, necessário, mensurável e justificável. O verdadeiro fator crítico de sucesso na integração entre tecnologia e negócio. Portanto, faça como eu: acredite no ROI da segurança.

*Marcos Sêmola é MBA em Tecnologia Aplicada, Bacharel em Ciência da Computação, Gerente de Produto e Consultor de Segurança da Módulo Security Solutions S.A.
msemola@modulo.com.br*