85 – Março 2007

10 lições sobre como perder dinheiro com projetos de segurança

Aprender com a própria experiência é importante, mas saber tirar lições dos erros alheios pode ser um diferencial e colocá-lo em vantagem. Assim, compartilho 10 lições que julgo valiosas para qualquer empresa ou gestor de segurança da informação.

1. Não envolver as pessoas
   Ignore as pessoas se quiser que seu projeto fracasse. Não procure saber a opinião delas, não mapeie seu entendimento sobre proteção da informação, não estude seu ambiente de trabalho, requerimentos e não conte com elas como parte do projeto. Este é o caminho mais curto para perder dinheiro e estabelecer um processo de segurança pobre e ineficaz.

2. Não integrar as áreas
   A informação está mais distribuída e seu manuseio, transmissão, armazenamento e descarte ocorrem através de meios cada vez diversificados. É, portanto, um desafio multidimensional que envolve pessoas, processos, tecnologias, além de agentes internos e externos, e não tratar o problema com coletividade é o primeiro erro. Não integrar os departamentos e considerar aspectos legais, físicos, éticos, políticos, técnicos e de negócio de forma integrada é a melhor forma de começar o jogo perdendo.

3. Não comunicar
   Como em todo processo complexo, não comunicar objetivos, requerimentos, inputs, outputs, progressos e as lições aprendidas ao longo do projeto pode antecipar o gosto amargo de uma iniciativa mal sucedida. Não comunicar eficazmente, ou seja, não estabelecer freqüência, consistência e adequação ao público, faz que com os pró ativos tornem-se neutros e os neutros tornem-se reativos.

4. Não estabelecer parcerias
   Um projeto de segurança da informação não é uma porção de terra cercada por água. Os problemas são multifacetados, seja processualmente, seja tecnicamente, e não estabelecer parcerias internas com outras áreas, assim como parcerias externas com empresas do mesmo setor e fornecedores de solução é anunciar o fracasso antecipado do projeto.

5. Não lutar por orçamento compatível
   Projetos de segurança podem assumir proporções gigantescas. De qualquer forma, quer seja pequeno ou grande, não entender bem os custos diretos e indiretos do projeto e com isso, não solicitar e lutar por um orçamento compatível vai proporcionar uma sensação indescritível no fim. O que deveria funcionar não vai funcionar e surgirá uma percepção geral de perda de tempo e dinheiro por conta de um projeto mal acabado ou simplesmente inacabado.

6. Não assumir suas fraquezas
   Super-homens e super-equipes não existem, ao menos na área de segurança informação. Pela diversidade de matérias envolvidas, dificilmente você e sua equipe deterão todo o conhecimento e experiência necessários para resolver ou endereçar todos os potenciais problemas. Não acreditar nisso e se julgar auto-suficiente é o primeiro degrau para o fracasso e a conseqüente perda de dinheiro.

7. Não atuar hoje pensando no amanhã
   Em geral, iniciativas de segurança precisam dar resultados no curto prazo acompanhando a velocidade de crescimento dos riscos. Mas agir com a cabeça no hoje sem enxergar e se alinhar com o amanhã pode tornar seu projeto perecível, e além de não preservar os investimentos, poderá fazê-lo começar do zero quando este ciclo de projetos terminar.

8. Não acreditar em idéias novas
   Não se pode esperar resultado diferente se tudo for feito da mesma forma. Assim, se o objetivo for estar à frente, se antecipar aos problemas e estar mais preparado para aqueles ainda desconhecidos, será preciso pensar "fora da caixa". Não agir preventivamente e não acreditar em idéias e formas novas de fazer a mesma tarefa pode não provocar maiores perdas, mas também não produzirá ganhos.

9. Não valorizar os bons profissionais
   O elemento humano é fundamental para qualquer projeto, mas definitivamente os profissionais de segurança têm valores diferentes em função da experiência, formação e dedicação. No jovem mercado de segurança da informação, poucos têm cabelos brancos e uma longa lista de projetos e certificações. Desta forma, não reconhecer as diferenças, valorizando e retendo os profissionais experientes enquanto paralelamente acredita e investe no potencial dos novos, pode colocar a continuidade e credibilidade de seu projeto em risco.

10. Não estar preparado para falhar
    Falhar é da natureza humana e uma realidade para o campo da tecnologia e segurança da informação. Não reconhecer e respeitar a possibilidade de falha é sustentar uma falsa sensação de segurança que resultará em frustração seguida de prejuízo e perda de tempo e dinheiro.

Marcos Sêmola *é Diretor de Operações de Security & Information Risk da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, certificado CISM, BS7799 Lead Auditor, Membro da ISACA, ISSA, CSI e fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV, Pós Graduado em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Premiado SecMaster® em 2003 e 2004, tornando-se membro da comissão em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br*