

49 – Julho de 2003

Change Management: a chave para “vender” segurança internamente.

Não é possível negar. O capital humano é determinante para garantir o sucesso de qualquer iniciativa empresarial com o objetivo de mitigar os riscos de segurança da informação e transformar as metas do Plano Estratégico de Segurança em ações reais.

É bem verdade que não faltam motivos, seja pela complexidade seja pela extensão, para se perder o foco e disparar ações desconexas ou tendenciosamente tecnológicas julgando serem suficientes para tranquilizar o CEO e acalmar os ânimos dos investidores.

Felizmente, muitas empresas estão no caminho certo e considerando os aspectos humanos como, ao menos, tão importantes quanto os ativos físicos e tecnológicos. Estão avaliando os riscos, planejando atividades e implementando controles à partir da identificação de vulnerabilidades, ameaças e impactos que relacionem por exemplo: o nível de cultura de segurança do funcionário; favores motivacionais; seu comprometimento com a missão da empresa e principalmente, seu preparo para as tarefas mais cotidianas que manipulam, armazenam, transportam e descartam informações sensíveis e valiosas para o negócio.

Estamos diante de um tremendo desafio para executivos e gestores especializados como: Chief Security Officers, que buscam encontrar uma equação de ROI equilibrada e capaz de tornar seus sistemas mais disponíveis, sua infra-estrutura mais tolerante e performática, seu ambiente físico mais segmentado e resistente a acessos não autorizados, e principalmente, garantir comportamentos seguros de seus usuários a partir da construção de uma cultura de segurança enraizada.

Formar cultura é o ponto chave! Pois por mais que um processo que manipule informações seja fisicamente e tecnicamente perfeito, sob a ótica da segurança, se em algum momento houver intervenção humana, ele estará potencialmente comprometido. Não que estejamos duvidando da competência e capacidade dos usuários, mas pelo simples fato de estarmos diante de uma “máquina” imprevisível e que pode errar.

Teoricamente, as regras do seu firewall irão se comportar exatamente como foram definidas, seu servidor de autenticação irá autorizar usuários só e somente só se estiverem cadastrados, a porta do data center permanecerá fechada se assim o quiser, mas seu usuário pode não ser tão amável, compreensivo e comprometido com a política de segurança da empresa em um determinado momento por conta de outro número indeterminado de motivos. A imprevisibilidade do capital humano é fator crítico para qualquer processo de segurança da informação.

É verdade que errar é humano e que não existe solução definitiva para comportamentos perigosos, mas há muito para se fazer no sentido de minimizar estes riscos. Eles refletem, entre outras coisas, a falta de percepção dos benefícios proporcionados pela segurança da informação, o medo da mudança, a ação desesperada de um usuário com auto-estima baixa

ou simplesmente a falta de treinamento. Por tudo isso, é justo nesta fase que todo projeto de segurança da informação deva contar com o apoio das atividades de Change Management.

É fácil compreender a resistência. Por definição, os controles de segurança tendem a reduzir a mobilidade do usuário no acesso a ambientes físicos, aumentar os critérios de autorização para acessos lógicos, gerar “burocracia” para manuseio, armazenamento, transporte e descarte de informações e ainda dar a sensação ao usuário de estar sendo monitorado e assim sujeito à repreensão de qualquer ordem. Por isso, ações paralelas de esclarecimento e envolvimento são fundamentais para “quebrar o clima”.

Procurando ser prático, é possível dizer que um projeto de Gerenciamento de Mudanças deve se cercar de artifícios para envolver os usuários, tornando-os participativos. Deve comunicar as mudanças, sinalizar a necessidade de apoio e principalmente realçar os benefícios de interesse comum, como por exemplo, a segmentação de responsabilidades, a redução de riscos dos processos e a própria continuidade do negócio, afinal, sem negócio não há posto de trabalho.

Principais elementos e atividades de um projeto de Gerenciamento de Mudanças:

- Avaliação do nível de comprometimento dos usuários com a empresa.
- Avaliação do nível de cultura de segurança da informação dos usuários.
- Mapeamento dos principais executivos e formadores de opinião.
- Identificação da percepção de importância da segurança para os executivos.
- Ações de envolvimento dos executivos a fim de realizar mudanças de percepção.
- Identificação da percepção de importância da segurança para os usuários.
- Plano de Ação para transformar reativos em neutros ou pró-ativos.
- Seminários de sensibilização e nivelamento de expectativas.
- Comunicado oficial da alta direção demonstrando comprometimento com a segurança.
- Programa de comunicação das mudanças.
 - o Selecionar mensagens chaves
 - o Selecionar veículos de comunicação corporativa
 - Curso
 - Palestra
 - Seminário
 - Workshop
 - Game
 - Email
 - E-learning
 - Wallpaper
 - Mousepad
 - Banner
 - Revista
 - Portal Web
 - Brinde
 - Concurso
 - etc

- o Segmentar o público alvo para adaptar a forma de abordagem.
- Implementação das ações de comunicação com a adoção dos veículos selecionados.
- Medição dos indicadores de resultado para os diferentes públicos.
- Ajustes das próximas ações com base nos indicadores de resultado.

Experiências recentes em que se associou atividades que promoveram alterações em processos e estruturas, com ações de gerenciamento de mudanças e expectativas, revelaram grande ganho de performance e maximização dos resultados. Fundamentalmente, um projeto de Change Management consegue converter reativos em pró-ativos, funcionários passivos em ativos e, principalmente, transformar a natural carência de capital humano disponível em uma *task force* que some esforços. Seja por movimento voluntário baseado na motivação, seja por movimento involuntário baseado na responsabilização, com ações dessa magnitude, todo projeto provocador de mudanças tende a se potencializar e resultar em um melhor retorno sobre os investimentos. Quando o foco é segurança da informação, este ganho fica ainda mais visível. É importante compreender que ninguém gosta de ter de fazer ou seguir algo sem estar certo de sua importância, de seus benefícios e o valor de sua participação, por menor que seja. Este é um dos princípios do Change Management. Assim sendo, passe a considerar esta atividade em seus planos de trabalho. Pode parecer uma despesa em uma análise preliminar, mas logo verá os resultados positivos de poder contar antigos “inimigos”, trabalhando agora do seu lado e em busca do mesmo objetivo.

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