

105 – Novembro de 2008

Quando menos é mais.

A indústria da tecnologia vem hipnotizando os usuários, fazendo-os trocar o que lhes parece bom e funcional hoje, pela promessa de algo melhor, sem antes mesmo descobrir como tirar o máximo proveito do que já possuem, ou ainda, sem se dar conta de que o produto que possuem já os atende plenamente.

O mesmo sentimento parece tomar conta de mim no campo da segurança da informação, o que vem ganhando volume ano a ano. Os lançamentos de novos produtos e soluções ocorrem em grande escala e tomam a forma de uma grande onda que vai varrendo os continentes. Ao mesmo tempo vemos grupos de estudiosos e engajados profissionais debruçados sobre suas mesas procurando caminhos alternativos, novas metodologias, novas ferramentas e por vezes, novas maneiras de se fazer a mesma coisa. Novos cursos, novas certificações, livros, seminários e treinamentos prometem a cura e pregam a palavra da salvação diante de tantos hackers, invasões e fraudes.

Tudo bem. Pareço meio desorientado depois de tantos anos fazendo exatamente o que descrevi acima, mas tudo isso me veio como um momento de lucidez, ou não, com diria Caetano, em que nitidamente vejo repetido o movimento da indústria da tecnologia. Onde antes mesmo de se resolver os mais básicos problemas, já se procura atacar os mais complexos e assim, se mantém o ciclo vicioso da busca incessante pelo mais. Não estou, de maneira alguma, negando o valor do estudo, da busca pelo aprimoramento, nem tão pouco o valor da transferência de conhecimento ou da qualificação profissional, mas sim a maneira como isso tem sido conduzido e o impacto dessa conduta nas organizações.

No exercício de funções de gestão de governança, risco e conformidade nos últimos anos, me vi por vezes rodeado por grandes problemas quando na verdade os menores deles, e possivelmente os principais causadores dos grandes problemas, sequer foram endereçados apropriadamente.

Quando então se discute gerenciamento de identidades, por exemplo, sem sequer se certificar de que os problemas com a criação, a manutenção e o comportamento do usuário na utilização de senhas foram controlados.

Quando então se discute criptografia na transmissão de dados, sem sequer se certificar de que chaves deixem de ser compartilhadas e relatórios deixem de ser esquecidos nas impressoras e nas salas de reunião.

Quando então se discute uma nova metodologia de desenvolvimento de software, sem antes se certificar que dados de produção não sejam mais utilizados em ambientes de teste.

Quando então se discute a adoção da nova geração de filtros de conteúdo, sem nem sequer saber ao certo o que fazer com os alertas já emitidos por seus precursores.

Ou ainda, quando se discute uma abordagem integrada de governança, risco e compliance, por exemplo, sem se certificar da existência de um alicerce baseado em uma linguagem comum como COBIT, para permitir a apropriada fusão e gestão dos controles.

Enfim, quando finalmente se discute o mais alto nível da proteção da informação, sem se dar conta de que muitas vezes, para proteger o negócio, não é mesmo preciso ir tão longe. Onde definitivamente a manutenção da indústria da vulnerabilidade não importa e o que chamamos de menos é na verdade, mais.

Marcos Sêmola é Global IT GRC Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. É ainda fotógrafo Getty Images com trabalhos publicados no Brasil, Estados Unidos, França, Inglaterra e Holanda www.s4photo.co.uk Visite www.semola.com.br ou contate marcos@semola.com.br

Nota: Este artigo expressa exclusivamente a opinião pessoal do autor, não representando necessariamente a opinião da empresa citada.