Por Emerson Siécola de Mello (*)

Quando ouvimos sobre segurança da informação, automaticamente pensamos em TI – Tecnologia da Informação. Na verdade, segurança da informação vai muito além de TI.

Informação é todo e qualquer ativo, dado ou conteúdo desenvolvido e/ou gerenciado, os quais devem ser protegidos de forma adequada e compatível com a missão da organização. Já por segurança da informação, temos os procedimentos de proteção das informações contra ameaças à sua disponibilidade, integridade e confidencialidade, de modo a se evitar riscos e vulnerabilidades, visando preservar a sua estrutura e assegurar a continuidade dos negócios.

Vale lembrar, ainda, que a transmissão da informação se dá por diversos meios: e-mail, papel, voz, pen drives, CDs, DVDs e por aí vai. Ou seja, as vulnerabilidades estão por toda parte!

Além destas possibilidades de transmissão da informação, ainda temos as situações de home office, acesso remoto, representação por terceiros, grandes volumes de base de dados, procedimentos inadequados de descarte de informações, compartilhamento de senhas, utilização de equipamentos pessoais no ambiente corporativo, bem como deficiências de segurança física e lógica. Isso só para começarmos a refletir sobre os cuidados necessários no gerenciamento e segurança da informação.

Na outra ponta das preocupações sobre o tema, lembremos que, sob a justificativa da liberdade de expressão, falhas de segurança da informação no ambiente corporativo podem ser o meio para cometimento de uma série de crimes como calúnia, difamação, favorecimento à prostituição, incitação ao crime, pedofilia, discriminação, revelação de segredo profissional, dentre outros, todos descritos no Código Penal, conforme bem citados na edição da Revista Eletrônica da CAASP, edição deste mês de Agosto.

Só para colocar um pouco mais de “lenha na fogueira”, não nos esqueçamos dos aspectos de produtividade: você sabe quais os programas utilizados pelo colaborador? Quais terminais ele utilizou? E em que ele trabalhou? Que sites acessou? Quanto tempo ele ficou conectado nas redes sociais? E as questões trabalhistas? Interesses pessoais, empreendedorismo virtual, sites indevidos e a produtividade do dia, do mês, do ano, jogada na lata do lixo. E sabe quem paga essa conta? A empresa. Pior se ela for a sua empresa!

O que fazer? Proibir acessos? Restringir? Liberar?

Já que em algum momento comentei sobre terceiros, quero registrar a percepção de má gestão do risco de segurança da informação também para os terceiros, mesmo em um ambiente altamente profissional, pois via de regra, “esperam” auditorias ou punições para investir em prevenção. Mas daí as perguntas: até onde posso controlar os terceiros? Quais as “áreas cinzentas”? Minha empresa está sujeita a possíveis danos colaterais?

Para não só evitar problemas, mas também para conscientizar colaboradores e terceiros, em todos os seus níveis, é necessário disciplinar condutas, prover treinamento adequado e conscientizar as pessoas continuamente sobre os riscos e perigos relacionados à segurança da informação e suas consequências.

As atividades de segurança da informação fazem parte das atribuições de qualquer compliance officer, e estão inseridas no contexto de gestão de riscos, no sistema de controles internos, no padrão normativo por meio de políticas e procedimentos, na confiabilidade das informações e reportes periódicos, bem como na aprovação e adequação de novos produtos.

A informação é um dos maiores patrimônios das empresas e as ameaças são as mais diversas e estão em constante evolução. Logo, é necessário identificar e tratar as vulnerabilidades, evitando os riscos desconhecidos.

Por fim, a confiança dos clientes é consequência da credibilidade e as atitudes dos colaboradores e dos terceiros definem a imagem das organizações.

É o momento de amadurecer e aprender! Governança da segurança da informação e práticas de compliance caminham juntas no trajeto de sobrevivência dos negócios.

(*) **Emerson Siécola de Mello** é Advogado Especialista em Compliance e Gerenciamento de Riscos Corporativos.

Fonte: Instituto Compliance Brasil, em 09.09.2015.