EMPREGADO PODE LEVAR AS INFORMAÇÕES DA EMPRESA AO SER DEMITIDO?

Em matéria publicada na InformationWEEK: Pesquisa da Symantec revela que perto de 70% dos empregados que deixaram suas empresas recentemente ou foram demitidos afirmam que companhias não protegem dados confidenciais.

Esta informação é extremamente preocupante, pois trata-se de pesquisa realizada nos Estados Unidos, Reino Unido, França, Brasil, China e Coreia do Sulm envolvendo mais de 3.3 mil pessoas.

O fato não é surpresa, pois no Brasil por experiência própria, na maioria dos casos apenas grandes empresas tomam as devidas precauções, incluindo capacitação e conscientização de seus empregados.

O "levar a informação embora" é mais comum do que se imagina e o pior é que os empregados nem sempre tem noção de que cometem uma infração, e afirmo, isto acontece em qualquer cargo.

Ocorre que ainda esta em fase de formação de cultura no que tange a prevenção de responsabilidade legal, é comum o brasileiro procurar ajuda só depois que o incidente ocorreu, no entanto é hora de mudar este cenário e pensar em ações preventivas.

Infelizmente nem todos percebem a importância do investimento em treinamentos, elaboração de Políticas e Normas Internas e na atualização de seus contratos. Os treinamentos/palestras devem abordar questões jurídicas de responsabilidade de cada parte, ou seja, empregado, empregador, parceiros, clientes, etc, acaba por prevenir um passivo razoável em demandas jurídicas, ou seja, evitar incidentes é mais barato do que deixar que se materializem.

O "levar a informação embora" é mais comum do que se imagina e o pior é nem sempre os empregados não tem noção de que cometem uma infração, e afirmo, isto acontece em qualquer cargo.

A situação ainda piora quando ele além de levar as informações a utiliza em seu novo emprego, dependendo do caso, o vazamento de informação pode caracterizar crime de concorrência desleal e responsabilizar as duas partes, a pessoa que as entregou e a empresa que a utilizou.

E será que a empresa está preparada para a devida coleta de provas?

Nem sempre a empresa está preparada para a coleta segura e lícita de provas, por exemplo, se as provas foram coletadas por monitoramento e constatou-se que as informações foram repassadas por email. Havia aviso de monitoramento? Esse monitoramento poderá ser utilizado?

As situações são as mais diversas, motivo pelo qual é preciso de acompanhamento jurídico especializado, para que o " feitiço não se vire contra o feiticeiro".

Caso o incidente já tenha ocorrido, a empresa deve ser orientada em relação ao que tem em mãos e ao que pode ser feito, após ter o embasamento legal e conhecimento das devidas consequências para todas as partes deve tomar a decisão do caminho a seguir.

Como evitar que estes problemas ocorram?

É preciso criar as regras e dar-lhes publicidade, ou seja, criar Política e Norma de segurança da Informação, trata-se de documento jurídico que define o que o empregado pode ou não fazer no que se refere ao uso das informações da empresa, ao uso das tecnologias que disponibiliza, entre outros.

Tais documentos norteiam as regras e requisitos técnicos de Segurança da Informação da empresa, geralmente elaborados com base na ISO 27001 e 27002 – Normas Técnicas de boas práticas Internacionais.

Ressaltamos, o empregado deve tomar ciência das regras.

Mas ressaltamos que os referidos documentos carecem e merecem a elaboração ou pelo menos a revisão por advogados que entendem de tecnologia, pois muitas vezes a equipe interna acaba por elaborar uma " juntada – um pouco daqui e um pouco de lá " com diversos modelos, mas que nenhum foi desenvolvido especificamente para seu negócio. Por exemplo, Hospital, educação, fundição e industrias automobilísticas são segmentos bem diferentes e merecem detalhamentos específicos.

Além das Políticas e Normas, recomendamos a publicidade de tais documentos, devendo ser levado aos colaboradores de forma didática que facilite seu entendimento, ou seja, cartilhas, palestras, treinamentos. No entanto ressaltamos que é necessário que as ações sejam continuadas, pois para mudança de cultura não basta uma única palestra ou um pedido de leitura.

Além disso, é necessário que as empresas se atentem à necessidade de atualização de seus contratos, seja de seus colaboradores direto ou terceirizados. Cláusulas sobre confidencialidade, responsabilidade no uso dos recursos tecnológicos e outras devem ser observadas com detalhes.

A matéria da InformationWeek acaba por indiretamente fazer uma alerta aos gestores e reforçamos aqui a necessidade de respaldo legal em suas ações e de se instaurar um projeto de Segurança da Informação.

Dicas Legais:

- Crie um Projeto de Segurança da Informação;
- Mencione na norma se haverá monitoramento de e-mails, sistemas, etc;
- Atualize seus contratos;
- Promova ações de conscientização para seus colaboradores;
- Promova integração das áreas TI e RH;
- Deve existir procedimentos para desligamento de empregados de forma que TI seja imediatamente avisado para bloqueio de acessos;
- Redija um termo de responsabilidade e confidencialidade;
- outros.

Link para matéria da InformationWeek - http://informationweek.itweb.com.br/12859/ex-funcionarios-acham-normal-levar-dados-corporativos-apos-demissao/

Cristina Sleiman é advogada e pedagoga, mestre em Sistemas Eletrônicos pela Escola Politécnica da USP e com extensão em Direito da Tecnologia pela FGV/RJ, extensão Educador Virtual pelo Senac São Paulo em parceria com Simon Fraser University. Sócia do escritório Cristina Sleiman Sociedade de Advogados, professora de Pós Graduação na Faculdade Impacta de Tecnologia, responsável pela coordenadoria de Prevenção de Crimes de alta tecnologia no ambiente corporativo na Comissão de Crimes de Alta Tecnologia da OAB/SP. Co-autora do audiolivro e livro Direito Digital no Dia a Dia publicado pela Saraiva. www.cristinasleiman.com.br / cristina@sleiman.com.br.

/2013