Como proteger dados, os ativos mais importantes da empresa

Palavra do gestor

Cristina Maria de Fiori

A informação é considerada atualmente um dos ativos mais valiosos de uma empresa. A forma como os dados são coletados, usados, armazenados e, por fim, preservados, vem ganhando enorme relevância nas organizações, justamente pelo valor que eles assumiram nos últimos anos e pelos crescentes casos de ataques às informações de pessoas físicas e jurídicas em evidência pelo mundo.

Em maio de 2017, diversas companhias de pelo menos 150 países, sofreram um ciberataque criminoso em massa, que sequestrou computadores e impossibilitou que colaboradores obtivessem acesso aos sistemas e dados. Os prejuízos financeiros foram amplos, uma vez que atividades e processos foram interrompidos.

De acordo com a pesquisa "International Business Report" da Grant Thornton — The Global Impact of Cyber Crime, em 2016, os prejuízos globais decorrentes de ataques no meio digital foram de US$ 280 bilhões. Esses dados foram obtidos junto a 2.500 líderes de organizações provenientes de 36 economias. Para mitigar riscos de invasões virtuais, é fundamental contar com uma boa estratégia de proteção de dados, que fortaleça os sistemas corporativos, já que esses incidentes têm aumentado ao longo dos anos no mundo todo.

Fraudes também geram problemas graves e são comuns dentro das empresas. Boa parte delas é decorrente de acessos ilícitos a dados corporativos ou devido aos ataques virtuais, que capturam informações sigilosas. Além disso, muitas fraudes podem ocorrer como consequência de vazamentos de informações pessoais de clientes e colaboradores da empresa, especialmente após ataques virtuais.

Dados de contatos, números de documentos, senhas, entre outros conteúdos que estejam com criminosos podem ser empregados para roubos de identidades e acessos a sistemas sigilosos, trazendo sérias consequências às pessoas lesadas.

Como resultado, esses casos dão margem a processos judiciais contra a organização pela negligência e ineficácia no armazenamento e proteção das informações pessoais.

Para evitar problemas como esse, é necessário adotar uma série de cuidados, como atribuir a cada colaborador uma identificação intransferível. As senhas devem ser alteradas com determinada periodicidade e os acessos devem ser monitorados. Para os colaboradores que lidarem com informações pessoais, é fundamental ter muito claro o dever de confidencialidade

Com a entrada em vigor da regulação de GDPR (General Data Protection Regulation — Regulamentação Geral de Proteção de Dados), diretiva europeia relacionada à proteção de dados, as organizações podem enfrentar multas significativas de até 4% de sua receita anual caso haja algum descumprimento de seus dispositivos.

A GDPR tem o objetivo de estimular que empresas compreendam a dimensão dos seus riscos de privacidade de dados e adotem medidas apropriadas para reduzir o risco de divulgação não autorizada de informações privadas de clientes europeus ou pessoas residentes na União Europeia.

No Brasil, atualmente não existe uma legislação própria que seja relativa à proteção de dados, mas os fundamentos são encontrados na Constituição Federal, no Código Civil, no Código de Defesa do Consumidor e no Marco Civil da Internet, dentre outros diplomas legais. Em discussão, há o projeto de lei 5.276/2016 e o projeto de lei da Câmara (PLC) nº 53/2018, o chamado Projeto de Lei Geral de Proteção de Dados (LGPD). Inspirados na GDPR, visam regulamentar de forma mais robusta o tratamento e a proteção de dados pessoais no país, por meio da criação de um conjunto de obrigações e responsabilidades para indivíduos e entes públicos e privados, que coletam e utilizam tais informações. Trata-se de um incentivo a mais para começar a se preparar desde já.

Nesse sentido, muitas empresas, inclusive, já têm nas suas posições os chamados DPOs – Data Protection Officers, pessoas responsáveis por supervisionar toda a cadeia relacionada à coleta, uso, tratamento e proteção de dados.

É certo que qualquer regulamentação relacionada ao tema demandará um aumento significativo do nível de compliance em matéria de privacidade e proteção de dados, mas o maior desafio é a mudança na mentalidade corporativa, o estabelecimento de um "data protection mindset", isto é, uma nova abordagem que incorpore na espinha dorsal das empresas a importância de adotar uma maior abertura e transparência na coleta, uso, tratamento e proteção de dados de clientes e colaboradores, demonstrando assim que a empresa utiliza o grau de diligência necessário que essas informações necessitam.

Cristina Maria de Fiori é gerente de compliance e do jurídico na Claritas Investimentos
E-mail: comunicacao@claritas.com.br