

Por Ana Albuquerque - Head de linhas financeiras da WTW Brasil



Se antes ter uma boa estrutura para lidar e proteger dados era algo tido como um diferencial competitivo para as empresas, agora a Lei Geral de Proteção de Dados (LGPD) tem elevado o patamar e tornado isso um padrão que beneficia a todos.

Há um pouco mais de um ano, a Autoridade Nacional de Proteção de Dados (ANPD) começou a aplicar as sanções da LGPD. Isso quer dizer que as empresas que não estiverem em conformidade com a lei podem ter de enfrentar consequências que vão desde advertência; publicização da infração, que pode acarretar danos à imagem; suspensão do exercício da atividade; e até multas, que podem chegar a R\$ 50 milhões.

Mas apesar dos riscos financeiros trazidos pela fiscalização, ainda é baixa a adesão da LGPD por parte das empresas brasileiras. Uma pesquisa realizada pela consultoria ICPS Protiviti, em maio deste ano, mostrou que apenas 16% se adaptaram à legislação e 84% acreditam que não estão preparadas para se adequar à lei.

Os motivos vão desde os custos financeiros que envolvem a adaptação até a falta de mão de obra qualificada na área de tecnologia. As pequenas e médias empresas (PME) são, inevitavelmente, as mais desafiadas por conta das barreiras existentes quanto à estrutura e verba.

A verdade é que se pode realizar treinamentos e investir em softwares, mas, no entanto, sempre poderá existir uma brecha para os criminosos cibernéticos e, além do prejuízo relacionado aos

danos de ataque cibernético, as empresas ainda podem enfrentar os processos resultantes de eventuais vazamentos de dados, inclusive responder pelas penalidades impostas pela LGPD.

Para algumas lideranças, não é mais uma questão de o que fazer 'se' ocorrer um incidente de segurança cibernética, mas sim uma questão de 'quando' um ataque irá ocorrer.

O impacto do crime cibernético nas empresas pode ser significativo, resultando em tempo e recursos adicionais necessários para remediar as violações, além, é claro, da perda de produtividade devido à incapacidade da equipe de realizar seu trabalho. Por isso, gerenciar riscos é essencial para minimizar a exposição a um incidente de segurança cibernética.

Um importante instrumento é o seguro Cyber que concede cobertura para custos de defesa, multas e penalidades, processos administrativos e judiciais que eventualmente possam ser instaurados em função do vazamento de dados de pessoas físicas, conforme diretrizes da LGPD. Além disso, auxilia as empresas na investigação de vazamentos e respectiva potencialidade de danos a terceiros.

Por isso, as empresas precisam ter em mente que a conformidade com a lei é algo que deve ser cuidadosamente mantida, mas é essencial contar também com outros instrumentos para se proteger.

A LGPD tem representado um novo paradigma de responsabilidade e está forçando uma mudança de cultura dentro das empresas que é fundamental. A lei estabelece as bases para a confiança e a transparência, que se correlacionam com o aumento da satisfação do consumidor estimulando a tão necessária evolução e competitividade do mercado.

Fonte: Virta, em 14.10.2022