Por Dr. Antonio Penteado Mendonça

Os números variam de dezenas de bilhões a trilhões de dólares, depende do quadro escolhido. Entre os maiores desafios internacionais, os riscos cibernéticos ocupam lugar de destaque, ao lado das mudanças climáticas e das novas pandemias. A ordem de grandeza desses três grupos de risco é inimaginável e capaz de levar o caos a uma nação. Com certeza, o setor de seguros não tem tamanho para fazer frente a eles, ainda que faturando inéditos sete trilhões de dólares este ano.

Os riscos cibernéticos têm ocupado espaço nobre na mídia e nas redes sociais. A razão disso é uma nova modalidade de crime que já custou pelo menos dezenas de milhões de dólares. Ninguém fala quanto pagou, mas o tamanho das empresas que tiveram suas redes de informática "sequestradas" por hackers que exigem o pagamento de resgate para liberá-las e permitir a volta da empresa ao seu funcionamento normal não deixa dúvidas. A conta está cara e vai ficar bem mais salgada. A tendência é que os crimes cibernéticos ganhem muito mais espaço e se espalhem para campos mais devastadores do que os atuais.

Ninguém sabe direito o começo da história, imagine o seu fim! O que é certo é que números na casa dos trilhões de dólares têm sido citados regularmente para quantificar prejuízos já ocorridos em função de crimes cibernéticos de diferentes matizes. Além disso, a casa dos bilhões de tentativas de invasão também tem sido a base para o cálculo do que acontece neste campo, ao redor do mundo.

O Brasil, que não deve ser uma das maiores prioridades dos criminosos, sofre milhões de ataques todos os meses. Todavia, o empresário brasileiro ainda não deu a devida importância ao problema, mesmo com grandes empresas sendo vítimas da ação dos bandidos e ficando fora do ar durante dias, porque suas redes foram "sequestradas", o que as impede de operar.

Quando se lê o nome das empresas vítimas dos "sequestros" ao redor do mundo, duas coisas ficam claras: primeiro, o tema é extremamente recente, o que faz com que as áreas de segurança empresariais não atentem para ele; e, segundo, no curto prazo, a melhor forma de se proteger é contratar um seguro para riscos cibernéticos porque os hackers estão muito à frente e as medidas de segurança utilizadas são incapazes de deter suas ações.

Como este cenário tende a se manter constante, com os hackers na frente das medidas de proteção, a briga do gato e do rato deve se acirrar, especialmente pela intensa divulgação do assunto e a consequente atenção de outros potenciais criminosos, capazes de desenvolver novos tipos de ataques.

Mas os crimes não são a única ameaça cibernética. Recentemente, alguns acidentes, internos e externos, em empresas e órgãos públicos, deixaram vazar informações armazenadas em sistemas de dados envolvendo milhões de pessoas que, sem autorização delas, tiveram informações confidenciais abertas e, portanto, ao alcance de todos, mediante uma simples consulta à Internet.

Acidentes como esses causam prejuízos astronômicos. Os valores envolvendo vazamentos de dados confidenciais podem facilmente atingir a casa dos bilhões de dólares, suficientes para quebrar a maioria das empresas ao redor do planeta.

É evidente que a melhor maneira de impedir ações criminosas ou acidentes internos e externos é adotar medidas que inibam sua ocorrência. Acontece que, no mundo real, nada é absoluto e não existe a proteção definitiva. Furos, invasões, vazamentos, negligência, imprudência, imperícia, falhas de terceiros, casos fortuitos e força maior sempre existirão e serão parte da rotina das empresas, por mais precavidas e cuidadosas que sejam.

É para isto que existem os seguros para riscos cibernéticos. Sua missão não é impedir a ocorrência do evento, mas minimizar prejuízos que podem, inclusive, ameaçar a continuidade da empresa.

O Brasil tem apólices modernas dando cobertura para os riscos cibernéticos. É tempo das empresas brasileiras atentarem para o problema e tomarem as providências necessárias para reduzir sua exposição. Entre elas, o seguro é das mais eficientes.

Fonte: O Estado de São Paulo, de 27.09.2021.