Por Paulo Leão de Moura Jr.

 Aos poucos, empresários no Brasil começam a entender o perigo do risco cibernético às suas atividades. A demora no interesse acontece por falta de legislação brasileira regulando e responsabilizando as operações cibernéticas.

O mercado global de prêmios de seguro cibernéticos é estimado entre 3 a 3.5 bilhões de dólares. Em 2020 deve atingir algo em torno de 7.5 bilhões de dólares. Dos 3 bilhões mundiais, os riscos cibernéticos dos EUA representam algo em torno de 80%, o que comparado com 530 bilhões de dólares em prêmios de seguros americanos em 2016, é ainda bem pouco.

A demanda por seguros cibernéticos deverá aumentar consideravelmente na Europa por conta da Regulação de Proteção de Dados Gerais a ser introduzida em 2018. Talvez o mesmo venha a ocorrer no Brasil, caso aprovada pelo Congresso a regulação do mercado cibernético, ora em discussão no Legislativo.

Independente dessa futura legislação - onde regulação, obrigações, responsabilidades, multas etc. se tornarão lei – o risco em si, para toda e qualquer empresa operando com TI, é real com sinistros consequentes de perdas e danos ocorrendo com certa assiduidade em diversas empresas no Brasil como Dropbox, Sony, Linkedin, XP Investimentos, Ingresso.com, Hospital Sírio Libanês, ... entre outras.

Na análise de risco de cada empresa devem ser adotadas diversas medidas. A primeira sem dúvida seria a própria empresa efetuar uma avaliação técnica profunda de todo o seu sistema de TI. Essa avaliação e inspeção deveria ser realizada por técnicos capacitados, preferencialmente, independentes da empresa, tendo como objetivo aferir a qualidade do sistema, identificando as debilidades e ameaças a que está sujeito e definir as medidas de controle de risco, prevenção e segurança que devam ser aplicadas para torna-lo o mais seguro possível. Estabelecer também as normas e regras de atuação que possam minimizar a ocorrência de eventos negativos, internos e externos ao sistema de TI da empresa.

Uma vez realizada esta etapa, a segunda medida seria a análise do resultado da avaliação para definir se é necessária a transferência do risco para seguro. Aqui o principal é conhecer com profundidade as condições dos seguros disponíveis no mercado nas principais modalidades de coberturas existentes: a responsabilidade civil por danos a terceiros, os diversos custos inerentes a recomposição das perdas e danos cibernéticos e, finalmente, uma das coberturas mais importantes, a de lucros cessantes por penalização das operações. Essa aferição não pode nem deve ficar restrita às condições de cobertura. Deve incluir necessariamente as cláusulas de exclusão de cobertura e as demais que determinam as obrigações e deveres das partes, segurado

e seguradora, com a devida consultoria e assessoria de um corretor de seguro profissional.

Se dessa análise resultar a necessidade de ser realizado um seguro, julgo conveniente que o assunto seja tratado da seguinte forma, a saber:

1. Reuniões entre seguradora, corretor de seguro e segurado para apresentação do produto seguro a ser realizado. A seguradora deverá ser representada pelo técnico subscritor do risco cibernético e pelo responsável pelo setor de sinistros. O corretor é o responsável por coordenar a apresentação do produto pelos representantes da seguradora. A apresentação deverá fornecer um posicionamento único para o segurado. Ultimamente verifica-se uma clara divergência de interpretações entre o que informa o setor de subscrição / comercial e o posicionamento do setor de sinistros com relação às coberturas e demais condições da apólice com severas consequências na regulação de eventuais sinistros.

2. Permitir, com transparência absoluta, a inspeção de risco a ser realizada pela seguradora que examinará as condições do sistema de TI a ser coberto. Deve, no entanto, ser apresentado com a devida forma, as condições de controle de risco adotadas pelo segurado, tanto para a seguradora considerar a aceitação do risco quanto para avaliar adequadamente o prêmio cotado e proposto, dadas as melhorias de controle de risco.

3. Apresentado o seguro e realizada a inspeção, segurado, corretor e seguradora devem analisar a eventual necessidade da adaptação das condições e cláusulas da apólice aos processos efetivos do segurado, já do pleno conhecimento do todos. Essa medida define, por fim, o seguro a ser contratado pelo segurado.

Com essas medidas, atrevo-me a sugerir que os corretores deveriam realizar um protocolo de intenções assinado pelos participantes, contendo uma clara definição das condições, do processo e da regulação de sinistros. O objetivo é verificar a apresentação da seguradora, com seus setores de subscrição e de sinistro, e deixar claras todas as obrigações dos participantes na administração do seguro durante a sua vigência, e nas eventuais regulações de sinistros. Esse protocolo faria parte das condições do seguro da mesma forma que os questionários e inspeções de risco.

Essa ideia do protocolo não é novidade para o mercado. Na Europa e nos Estados Unidos é prática normal aos seguros corporativos, conforme apresentação feita pela Munich Re em seminário promovido pela Demarest Advogados. Sinceramente, não vejo o motivo do mercado não aceitá-lo e muito menos a SUSEP não autorizá-lo, caso seja necessária essa aprovação.Trata-se unicamente de implantar transparência aos processos de seguro, tendo em vista as ambiguidades contraditórias das cláusulas de seguro.

Finalmente, o mais importante é que os segurados enxerguem a grande ameaça em relação ao risco cibernético e procurem tanto corretores de seguros quanto seguradoras para atender as necessidades das suas empresas.

Dezembro de 2017.