Paulo Leão de Moura Jr.

É extremamente difícil, na situação em que nos encontramos neste país, na constatação de que vivenciamos um estado geral de corrupção, apresentar um artigo convincente sobre a problemática de risco e seguro. É bem verdade que o nosso setor de seguros, ao menos até agora, tem demonstrado estar alheio, que não participou nem participa de escândalos envolvendo propinas, delações, enfim, do infortúnio que assola nossa sociedade em seus valores básicos, na política e na economia.

Recentemente, o mundo sofreu um forte ataque cibernético com “hackers” invadindo sistemas em diversos países, com finalidade de ameaças de chantagem.

Já discutimos inúmeras vezes, a questão do risco cibernético e seu impacto nas empresas em geral. A meu ver, poucos se dão conta dos grandes riscos que enfrentam, especialmente quanto aos lucros cessantes e responsabilidade civil, dificilmente mensuráveis e os de danos materiais mais quantificáveis. Por outro lado, o nosso mercado, salvo as experiências de poucas seguradoras e o estudo de outras na possível implantação de produtos de garantia de riscos cibernéticos, não demonstra ter grande apetite pelo risco em questão. A maioria pretende apresentar produtos restritos às instituições financeiras e a empresas que armazenam muitos dados de pessoas físicas.

Da análise do risco cibernético é fácil concluir que atualmente as medidas iniciais mais importantes são a aplicação do gerenciamento do risco por parte do usuário. A parte essencial nesse gerenciamento são as questões de controle de risco, isto é, nas medidas de segurança e proteção dos sistemas escolhidos e na avaliação do real valor em risco, em especial, quanto ao lucro cessante. A minimização do risco mediante ações de controle de risco é que irá permitir melhores condições de negociação na colocação do risco no mercado segurador.

Nenhuma seguradora irá aceitar um risco cibernético amplo sem antes realizar profundo

“assessment” ou avaliação dos sistemas de cada segurado. A aceitação do risco vai depender exatamente dessa avaliação prévia, até certo ponto conflitante, pois em tese, permite o conhecimento o mais exato possível do risco do segurado e, consequentemente, permitindo uma análise razoável do que garantir e do que excluir.

Eventualmente, a solução para esse aparente conflito de interesses seria a realização dessa avaliação ou “assessment” por empresa independente, tecnicamente abalizada em TI e em gerenciamento de risco. Sua avaliação e medidas de controle de risco a serem adotados seriam pagas em partes iguais pelo segurado e pela seguradora.

É claro e evidente que o seguro cibernético terá que resultar de análises específicas e que as condições e cláusulas da apólice deverão ser acordados mediante negociação transparente entre as partes. Da mesma forma, as taxas e prêmios aplicáveis serão definidos caso a caso e, dificilmente, poderão ficar submetidos ao tipo de concorrência abusiva e predatória comum ao mercado brasileiro em outros ramos. Será difícil aos nossos segurados e seguradores entenderem que a taxação do risco cibernético espelha o resultado da análise de risco individual e as garantias efetivas a ser concedidas. O risco cibernético não pode ser tratado como um seguro de prateleira. Assim, temos mais uma dificuldade a ser ultrapassada na sua aceitação, na preparação adequada dos processos de “underwriting”.

Consideradas as empresas em geral, na verdade, os riscos que impactam severamente aos usuários de sistemas de informática são, ao meu ver, os seguintes:

√ Danos Materiais: danos causados a máquinas e equipamentos em geral, que atuam mediante sofisticados sistemas de informática, incluindo autodestruição, por atuação de hackers. Inclusos ainda os equipamentos que compõem a rede, o hardware e o software das empresas, inclusive e eventualmente, as despesas de recomposição dos trabalhos.

√ Lucros Cessantes: perdas e danos consequentes da destruição dos equipamentos ou da interferência na sua ação programada irão resultar em lucros cessantes com prejuízos que poderão ser, inúmeras vezes, bem superiores aos danos físicos. A própria perda das atividades por ataques aos sistemas, aos computadores e demais equipamento, poderá cessar totalmente as atividades empresariais e resultar nos lucros cessantes consequentes.

√ Responsabilidade Civil: perdas e danos causados a terceiros consequentes da paralisação da entrega de produtos e serviços não realizados e passíveis de cobertura. A polêmica que eventualmente surgirá sobre as reais responsabilidades de uma empresa por ações de terceiros que a impossibilitem de atuar e cumprir os seus compromissos é, a meu ver, bastante relativa. A obrigação da empresa está no fornecimento de produtos e serviços contratados. A quebra dessa obrigação será de sua responsabilidade, independente do motivo, e um ataque cibernético dificilmente pode ser considerado um evento fortuito ou de força maior. Outro aspecto a considerar é que, em relação à Responsabilidade Civil, os usuários dividem-se entre empresas em geral que operam os seus sistemas de informática e empresas que prestam serviços de implantação de sistemas de informática. Estas últimas tem uma responsabilidade profissional, inequívoca e óbvia em relação a seus contratantes, inclusive questões relativas ao lucro cessantes desses terceiros. As empresas que contratarem os serviços de informática terão que considerar, independente da exigência de garantia profissional do contratado, a necessidade de incluir a garantia de lucros cessantes contingente em seus seguros de RO Lucros Cessantes.

O que o mercado de seguros oferece em coberturas que possam minorar o impacto de perdas e danos em consequência da ocorrência de riscos cibernéticos, envolve essencialmente prejuízos causados a terceiros, ou seja, seguro de responsabilidade civil. Incluem, entretanto, algumas coberturas que julgo importantes. Além das coberturas de quebra de confidencialidade de dados, violação de publicações, danos morais, propriedade intelectual, são interessantes as coberturas que diretamente protegem o segurado e que não são, portanto, coberturas de responsabilidades

civis. São elas: cobertura de interrupção de negócios decorrentes do comprometimento da rede do segurado, isto é, lucros cessantes e despesas operacionais; a cobertura de prejuízos decorrentes de extorsão por terceiros que comprometem a rede e as coberturas de despesas diversas com perícia, gerenciamento de crises, custos com despesa; restituição de imagem; reposição entre outras.

Nesse contexto altamente técnico, qual será o papel do corretor de seguros profissional? Certamente, não o do tradicional intermediário de seguros. Cada vez mais, o gerenciamento de risco passa a ser atividade corrente e essencial aos serviços dos corretores de seguros. Isto em todos os ramos, mas certamente obrigatório no risco cibernético. Neste o corretor tem a primordial ação em assessorar o segurado na introdução, implementação e no acompanhamento dos sistemas de controle de risco, em negociar e definir as condições técnicas do seguro, os valores em risco, as condições de coberturas e exclusões de riscos, as franquias e as taxas aplicáveis,

Exemplifica o que foi mencionado anteriormente: o risco cibernético deve ser analisado em conformidade com as singularidades de cada segurado que deve ser objeto de estudo profundo e específico.

O que se faz necessário é que as importantes discussões sobre o perigo cibernético façam tanto os usuários quanto as seguradoras atentarem sobre o enorme risco potencial e que ofereçam efetiva e real suporte à cobertura desse risco.

Fonte: Revista Opinião.Seg nº 14 - Julho de 2017.