Risco cibernético: o que está coberto pelas apólices tradicionais?

O mercado de seguros contra riscos cibernéticos ainda está em desenvolvimento. Mas especialistas apontam que muitas das perdas criadas por tais riscos já são cobertas por outras coberturas existentes o mercado.

Uma das tarefas que as empresas que pensam em transferir riscos cibernéticos devem realizar, portanto, é avaliar que perdas já são cobertas por seus atuais programas de seguros, e quais estão excluídos nas apólices.

Para ajudar nessa missão, a Associação Internacional de Subscritores de Londres (IUA, na sigla em inglês) publicou um relatório que procura identificar exatamente o que está coberto ou não, em termos de riscos cibernéticos, nas atuais apólices de seguro.

A dificuldade já começa na identificação do que é um risco cibernético. O estudo define tal risco como uma ameaça tanto direta à empresa como a terceiros, e que pode ir desde extorsões e investigações regulatórias até lesões físicas ou mesmo morte de pessoas.

Por isso a variedade de danos causados pelas ameaças cibernéticas é ampla e pode muitas vezes estar cobertas por apólices em vigor.

A terminologia utilizada pelo relatório, elaborado em conjunto com o escritório de advocacia Norton Rose Fulbright, se baseia nas apólices existentes no mercado londrino, motivo por que podem não bater literalmente com os clausulados aprovados pela Susep, que muitas vezes são bastante peculiares ao mercado brasileiro.

A comparação, no entanto, pode ser útil para empresas que estão passando pelo processo de identificação de sua exposição cibernética.

Alguns exemplos

D&O

O relatório cita o caso hipotético em que um diretor de uma empresa perde um laptop com dados de dois milhões de clientes. A empresa notifica as autoridades, que lhe mandam entrar em contato com os clientes afetados, e o caso acaba vazando para a imprensa.

Como resultado, a empresa sofre danos reputacionais e o preço da ação cai na Bolsa de Valores. O diretor é então processado por acionistas por falhar na implementação de medidas de segurança cibernética. A empresa e o próprio diretor correm o risco de serem processados por violação da privacidade de seus clientes.

A empresa procura então acionar sua apólice de D&O para cobrir os custos legais envolvidos.

De acordo com o relatório, neste caso, a seguradora avaliará se o diretor perdeu o laptop enquanto executava suas funções corporativas. Caso estivesse utilizando o equipamento para fins pessoais, a cobertura poderia ser negada.

Em geral, porém, os custos legais das ações em questão não são excluídos das apólices D&O puramente por se tratarem de riscos ligados ao mundo virtual, segundo o relatório.

Responsabilidade Civil Profissional (PI)

As apólices de responsabilidade civil profissional, muito conhecidas no mercado como PI (Professional Indemnity), protegem as empresas em caso de litígio sobre a qualidade de um serviço ou acusações de negligência por parte de clientes. Empresas que participam de licitações públicas, por exemplo,

constituem um público-alvo desta linha.

O relatório afirma que, no mercado internacional, as apólices PI em geral não possuem exclusões relacionadas a riscos cibernéticos.

O estudo avalia o caso também hipotético em que uma empresa compromete a privacidade de um cliente ao enviar erroneamente, por email, informações confidenciais sobre ele para terceiros.

Como resultado, a empresa é acionada na Justiça tanto pelo cliente quanto por um órgão regulador que lida com o tema da privacidade da informação, e aciona sua apólice PI para cobrir os gastos legais.

De acordo com o IUA, a princípio, os custos legais das ações devem ser cobertas pela apólice, se o caso realmente se deu por negligência. Mas pode haver exclusões para o pagamento de penalidades, especialmente se forem impostas por um órgão regulador.

Por outro lado, caso o regulador demande a abertura de um processo de acesso aos dados do cliente afetado (conhecido na Inglaterra como Data Subject Access Request), é improvável que os custos envolvidos, que podem ser consideráveis, sejam cobertas pelo seguro de responsabilidade civil profissional.

Dados à propriedade e lucro cessante

Outro exemplo avaliado pelos autores do estudo é o caso de uma empresa industrial que possui uma cobertura de danos à propriedade e lucro cessante que, sob a sigla PDBI, é bastante comum no mercado de Londres.

Na suposição feita pelo estudo, a empresa sofre um ataque de hackers que danifica o equipamento de uma fábrica coberta pelo seguro, interrompendo a produção por 36 horas.

Líquidos corrosivos são liberados, causando estragos na fábrica, e forçando a realização de reparos que fecham a

unidade por mais algumas semanas.

Além disso, os servidores da fábrica são destruídos, eliminando informação de pesquisa e desenvolvimento altamente importante para a empresa.

A empresa aciona então sua apólice PDBI para cobrir tantos os danos físicos quanto os prejuízos causados pela interrupção de suas operações nos dois eventos.

Segundo os autores, caso a fábrica se localize, por exemplo, no Reino Unido, é improvável que a apólice cubra o lucro cessante no primeiro episódio, já que não houve destruição de propriedade, que é uma condição necessária para ativar a apólice PDBI em alguns países.

Além disso, essas apólices com frequência incluem exclusões a danos causados por alteração, destruição, perda, dano, eliminação e comprometimento de informações digitais.

Para piorar a situação, apólices PDBI também costumam ter exclusões ambientais, por exemplo relacionadas a danos causados por produtos químicos.

Este é um caso, portanto, em que poderia ter valido a pena haver contratado uma cobertura dedicada ao riscos cibernéticos.

Um outro exemplo é o caso de ataques terroristas realizados por meios cibernéticos. As apólices de terrorismo em geral incluem exclusões a este tipo de perda, observa o documento da IAU.

Para conhecer mais comparações, clique aqui para baixar o relatório completo, em inglês.