FABIO TORRES & ASSOCIADOS

TM LAW

Cyber Risks – O Seguro de Riscos Cibernéticos

Introdução

Não há dúvida de que o seguro de Riscos Cibernéticos oferece oportunidades consideráveis para Seguradoras interessadas em expandir suas carteiras e obter margens favoráveis de lucros em um mercado *soft* como o atual.

Em discurso proferido na reunião da AAMGA (*American Association of Managing General Agents*) em 28 de maio de 2015, John Nelson, Chairman do Lloyds, assinalou que cerca de US$ 2,5 bilhões em prêmios de seguros de Riscos Cibernéticos haviam sido subscritos no ano de 2014, dos quais nada menos que 90% por empresas norte-americanas[1]. Noves fora a alta concentração geográfica, o campo para expansão afigura-se gigantesco, considerando-se, a título de ilustração, que no Reino Unido apenas 2% das empresas têm tal seguro e que, mesmo no disputadíssimo mercado dos EUA, apenas 1/3 das empresas têm algum tipo de cobertura cibernética. Some-se a isto que, à medida que o reconhecimento e a reação a ameaças cibernéticas aumentam, também aumenta a expectativa de empresas quanto à contratação de um produto securitário que sirva à mitigação e transferência (ao menos parcial) das consequências resultantes dos riscos correspondentes. Não por outra razão, relatório da Price Waterhouse (PwC) estima que o mercado de seguros de Riscos Cibernéticos poderia crescer para aproximadamente US$ 5 bilhões em prémios anuais por 2018 e pelo menos US$ 18 bilhões em 2025[2].

Tal expectativa de crescimento se deve a que os ataques cibernéticos estão aumentando em frequência através do mundo – houve um crescimento de 48% em 2013, subindo para 42,8 milhões em 2014, o equivalente a 117.339 ataques por dia –, e assim também o custo de gerenciamento e mitigação de violações. A estimativa é de uma média de perdas por cada incidente da ordem de US$ 2,7 milhões em 2014 (um aumento de 34% comparativamente a 2013).

O apetite dos *underwriters* para uma expansão na oferta de produtos voltados especificamente para riscos cibernéticos tem se refletido na recente aprovação de novos produtos junto à

[1] https://www.lloyds.com/~/media/files/the%20market/operating%20at%20lloyds/lloyds%20cyber%20attack.pdf

[2] http://www.pwc.com/gx/en/insurance/publications/assets/reaping-dividends-cyber-resilience.pdf.

Superintendência de Seguros Privados – SUSEP, que vieram se somar aos (poucos) até então já existentes no mercado. Nosso Escritório teve a felicidade de participar da elaboração e aprovação de três desses produtos, colocando-se, uma vez mais, em posição de vanguarda na assessoria jurídica ao mercado segurador. Ainda é cedo para dizer quais serão os impactos comerciais do aumento do número de Seguradoras aptas à subscrição de riscos cibernéticos por um produto específico. Noutros países, o mercado ainda se ressente de uma precificação relativamente alta, que incorpora elementos de incerteza relacionados à pouca experiência na quantificação das perdas decorrentes de reclamações apresentadas por terceiros; no Brasil, há um entrave adicional à comercialização a considerar: a ausência de uma legislação protetiva específica, eis que o projeto de lei de proteção à privacidade de dados ainda tramita no Congresso Nacional (embora, deva-se dizer, a passos relativamente largos).

Não obstante as dificuldades, estudos demonstram que a Internet gera anualmente uma receita entre US$ 2 trilhões e US$ 3 trilhões, dos quais, veja-se, 15% a 20% são perdidos por conta de práticas criminosas[3]. E como fica o Brasil neste contexto? Pois bem, uma pesquisa de empresas brasileiras constatou que um terço haviam sido vítimas de crimes cibernéticos. Em fevereiro de 2012, um grupo que se autodenomina "Anonymous Brasil" lançou um “ataque de negação de serviço” (que explicaremos a seguir) contra *sites* financeiros brasileiros[4], incluindo o de Citigroup; noutro ataque, *hackers* comprometeram 4,5 milhões de *routers* DSL, incentivando os usuários a fornecerem informações pessoais sensíveis ou instalando *malware* em seus aparelhos[5]. Ataques se avolumam e, quando se tornam públicos, conquistam espaço significativo na mídia.

O fato é que, com o avanço da Internet e as mudanças acentuadas ocorridas no perfil das relações de consumo e dos sistemas de arquivamento e transferência de dados, eventos indesejados inevitavelmente se ampliarão em frequência e severidade e demandarão das empresas a adoção de mecanismos eficientes de pulverização de riscos. Em contrapartida, porém, os produtos securitários tradicionais se mostram insuficientes para atender à dinâmica dos custos e perdas decorrentes de um ataque cibernético. Esse descasamento entre um aumento exponencial dos riscos, de um lado, e a oferta ainda incipiente de cobertura, de outro, indubitavelmente tenderá a beneficiar aqueles Seguradores que se prontificarem a suprir a demanda crescente de seus Segurados.

Já se disse que “o comércio eletrônico emergirá como o maior risco corporativo do século XXI”[6]. Assim se dá porque, a cada evento, o ganho de escala proporcionado pelo uso massivo de sistemas

[3] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2.pdf

[4] Gerald Jeffris, “Citi Hit in Brazilian Hacker Attack,” The Wall Street Journal, February 4, 2012, http://online.wsj.com/news/articles/SB10001424052970203889904577200964142208498.

[5] Dan Goodin, “DSL modem hack used to infect millions with banking fraud malware,” Ars Technica, October 1, 201.

[6] David |R. Cohen & Roberta D. Anderson, Insurance Coverage for Cyber-Losses”, 35 Torts & Insurance, LJ 891, 892 (20000).

computadorizados conduz a uma expansão substancial no número de reclamações em potencial comparativamente à era "pré-internet", além do que despesas de contenção e custos de defesa sobem em escalas jamais vistas, dada a complexidade e o alcance de cada violação. As possibilidades, portanto, se afiguram promissoras, porém não se pode perder de vista que o seguro de Riscos Cibernéticos guarda características únicas que reclamam conhecimento especializado de subscritores, analistas de sinistros, reguladores e advogados.

Este artigo é uma tentativa – que esperamos seja bem-sucedida – de compartilhar nossa experiência com todos os interessados.

O desenvolvimento do mercado de seguros de Riscos Cibernéticos

Apólices de Seguro de Riscos Cibernéticos contêm coberturas de "primeira parte" e de "terceira parte".

Coberturas de "primeira parte" – ou seja, destinadas a "danos diretos" – geralmente pressupõem a ocorrência de um dano, perda ou destruição física ou material a um item patrimonial tangível e coberto, decorrente da materialização de um risco também coberto. Como ataques cibernéticos, no mais das vezes, envolvem danos ou perdas imateriais, de conteúdo informacional, não é difícil ver que boa parte das Condições Contratuais das Apólices tradicionais de *property* não se aplica a eles.

De fato, imagine-se, por exemplo, que um "ataque de negação de serviço" coloque um website "fora de serviço" por determinado período de tempo, todavia sem causar-lhe um dano, perda ou destruição: o website, neste exemplo, permanece íntegro, de modo que não se poderia cogitar de um dano à propriedade tangível; mesmo um vírus pode infectar um sistema de computação e não lhe causar um dano físico, mas exigir o dispêndio de vultosa soma para sua limpeza.

É bem verdade que outras Apólices – como as de Responsabilidade Civil Profissional (E&O), Fidelidade, Fraude Corporativa e Sequestro (K&R) – oferecem cobertura para eventos de natureza cibernética, porém pior do que não ter cobertura alguma (e sabê-lo) é crer que ela exista e descobrir depois que a Apólice tem "*gaps*" que a tornam ineficaz para uma variedade substancial de acidentes cibernéticos. Um Segurado que se depare com um pedido de "resgate" sob a ameaça de destruição de seus arquivos ou servidores não terá cobertura em uma Apólice de K&R que restrinja tal cobertura a uma ameaça de danos corporais. Uma Apólice de Fidelidade provavelmente cobrirá danos decorrentes de atos desonestos praticados por um empregado ou colaborador que destrua o sistema de computação do Segurado, mas presumivelmente excluirá os lucros cessantes daí

decorrentes. Apólices de Lucros Cessantes, por sua vez, são normalmente contratadas como secundárias à cobertura para Danos Materiais e, portanto, não prescindem da ocorrência de um dano material, por vezes restrito à propriedade tangível. Como se vê, as Apólices tradicionais oferecem uma cobertura limitada aos riscos cibernéticos.

Ataques cibernéticos também são aptos a causarem danos a terceiros, requisitando a intervenção de coberturas de "terceira parte" (i.e., de "danos indiretos" ou "de responsabilidade"). Neste caso, na ausência de um Seguro específico para Riscos Cibernéticos, o Segurador recorrerá a suas Apólices de Responsabilidade Civil Geral, Profissional (E&O – em especial Technology E&O), de Administradores (D&O) ou de "Mídia", conforme seja o caso. Os danos, normalmente, dirão respeito à violação da privacidade, ao uso indevido de informações, ou à violação de direitos de propriedade intelectual. Muitas Apólices de Seguro de Responsabilidade Civil, porém, terão exclusões para lucros cessantes que não sejam decorrentes de um dano físico ou material (e nem sempre um ataque cibernético produzirá um dano físico ou material), bem como para danos decorrentes da comercialização e/ou atividades do Segurado relacionadas à transferência eletrônica de dados, web, uso de computadores e/ou de programa de computação, vírus de computador, ou da falha ou mau funcionamento de qualquer equipamento e/ou programa de computador e/ou sistema de computação eletrônica de dados. Ademais, há uma tendência inequívoca e irreversível à ampliação do rol de exclusões das Apólices de Responsabilidade Civil Geral em relação a riscos relacionados à responsabilidade por danos ambientais, à violação de direitos de propriedade intelectual e, no presente caso, a responsabilidade por eventos de violação de segurança ou privacidade de dados, impulsionando os Segurados à contratação de produtos que lhes provejam coberturas mais específicas, sujeitas a procedimentos de *underwriting* próprios e mais detalhados[7].

Além disto, tampouco se pode desconsiderar o fato de que a complexidade e o alcance das repercussões advindas de um ataque cibernético podem levar à exaustão dos limites máximos de indenização antes mesmo que qualquer terceiro apresente uma reclamação; daí que, para mitigar os prejuízos (sobretudo à sua imagem e reputação profissional), os Segurados devem se mostrar eficientes na adoção de medidas emergenciais de contenção e investigação. A experiência, contudo, revela que os adquirentes de seguros de Riscos Cibernéticos, no mais das vezes, não dispõem da expertise necessária ao processo de tomada de decisões em uma situação de crise, de modo que a assistência de uma Seguradora especializada – tanto diretamente, como por meio de profissionais especializados por ela selecionados com antecipação – pode constituir um instrumento valioso. Tal oferta de profissionais é inteiramente distinta daquela de que trata a Circular SUSEP 310/2005 ou a revogada Carta-Circular/DETEC 03/2006 e, longe de ser coibida pela SUSEP, deveria ser compreendida como um aspecto elogiável do produto.

[7] Este fenômeno foi analisado por Kenneth Abrahams em "The Rise and Fall of Commercial Liability Insurance", 87 VA. L. VER. 85, 86-101, 104-105.

Seguros de Riscos Cibernéticos surgem, por conseguinte, neste vácuo de coberturas e serviços não preenchidos pelos produtos tradicionais, e, de maneira geral, oferecem coberturas de "primeira parte" e "terceira parte", garantindo o interesse segurado quando a custos, despesas e perdas e danos ao seu próprio patrimônio, causados por um evento (ou ataque) cibernético, bem como quanto a perdas e danos que o Segurado venha a ser legalmente condenado a pagar em decorrência de reclamações apresentadas por terceiros prejudicados.

Riscos Cobertos

Conforme anteriormente exposto, um componente relevante da cobertura securitária constitui-se de custos e despesas realizadas pelo Segurado visando a interromper ou evitar um ataque cibernético, a contê-lo dentro de certos lindes, e a investigar sua autoria (estes custos são normalmente incorridos com especialistas "forênsicos"). Em certa medida, estes custos e despesas estão sujeitos a limites máximos de indenização específicos e, na sua maior parte, são efetuados emergencial e imediatamente após a constatação de um ataque ou evento cibernético, tendo por finalidade limitar os seus efeitos danosos (motivo pelo qual é possível enquadrá-los, na sua maior parte, como despesas de contenção, sujeitas a limites específicos).

Ademais, essas Apólices normalmente também cobrem os custos de defesa incorridos em processos administrativos sancionadores (movidos, por exemplo, perante órgãos reguladores, no caso de atividades reguladas, ou junto à própria autoridade encarregada da proteção à privacidade de dados, quando houver), judiciais e arbitrais que decorram do ataque ou evento cibernético, neste caso à semelhança do que ocorre em outras Apólices de Responsabilidade Civil.

Por sua vez, coberturas de "primeira parte" encontráveis em Apólices de Riscos Cibernéticos (como não existem formulários ou condições contratuais standard, as coberturas variam de Seguradora para Seguradora, conforme seja o foco adotado) usualmente se referem à (ao) (s):

(i) Perda ou dano de ativos digitais, tais como dados ou programas de *software*;
(ii) Lucros cessantes decorrentes da interrupção de negócios em função da inatividade da rede ou do sistema computacional;
(iii) Pagamento de "resgates" por extorsão praticada por terceiros que ameacem danificar a rede ou sistema ou divulgar ao público ou a concorrentes dados sensíveis sob a guarda, custódia ou controle do Segurado;
(iv) Despesas de notificação aos clientes cujos dados porventura tenham sido violados, quando houver uma exigência legal ou regulamentar para se notificá-los de uma violação à sua segurança ou privacidade;

(v) Danos à reputação decorrente de uma violação de dados que resulte em perda de direitos de propriedade intelectual ou mesmo de sua clientela;
(vi) Furto de dinheiro, valores mobiliários ou ativos;
(vii) Despesas incorridas com a "Gestão de Crises" e "Relações Públicas", tendo por objeto a garantia do interesse segurado quanto a despesas incorridas pelo Segurado na contratação de profissionais especializados;
(viii) Multas contratuais pela violação de acordos ou contratos que inibam a divulgação de informações sigilosas.

Ditas coberturas estão vinculadas à ocorrência de um ataque ou evento cibernético, sendo este o ato danoso ou o fato gerador, cuja definição será aquela constante na Apólice. Em regra, tais ataques dividem-se em dois grupos ou gêneros (cujas nomenclaturas variam de Apólice para Apólice) – (i) falhas ou violações da segurança de rede e computacional e (ii) atos de violação de privacidade. Ditos gêneros, por sua vez, desdobrar-se-ão em diversas espécies, que incluem ataques de negação de serviços, introdução de vírus informáticos, Cavalos de Tróia, *malwares*, *spywares*, *ransomwares*, entre outros. A caracterização da ocorrência de alguma dessas espécies de ataques ou eventos cobertos é o risco coberto que dará ensejo à cobertura da Apólice.

Conquanto não pretendamos exaurir o tema, passamos, a seguir, à descrição dos principais tipos de ataques ou eventos encontrados nas Apólices de Riscos Cibernéticos, segundo a terminologia correntemente adotada:

Ataque cibernético de negação de serviço (*Denial of Service* – DoS) – ocorre quando um website é bombardeado por milhões de e-mails a partir de uma "fonte" ilegítima, deste modo bloqueando o acesso ao website de usuários legítimos. Um DDoS é o mesmo que um DoS, apenas proveniente de diversas fontes.

Bluebugging – ocorre por meio de falhas de segurança em dispositivos Bluetooth; com equipamentos de captura de sinal Bluetooth, crackers podem roubar dados e senhas de aparelhos celulares ou notebooks que possuam a tecnologia habilitada.

Botnet – são computadores invadidos por um determinado *cracker*, que os transforma em um replicador de informações, tornando mais difícil o rastreamento de computadores que geram *spams* e aumentando o alcance das mensagens propagadas ilegalmente.

Compromised-Key Attack – são ataques realizados para determinadas chaves de registro do sistema operacional. Quando o *cracker* consegue ter acesso às chaves escolhidas, pode gerar logs com a decodificação de senhas criptografadas e invadir contas e serviços cadastrados.

Keylogging – são aplicativos ocultos instalados no computador invadido, que geram relatórios completos do que for digitado, servindo à captura de senhas e nomes de acesso de contas de email, serviços online e até mesmo *Internet Banking.*

Malware – qualquer aplicativo que acesse informações de um sistema computacional ou de documentos alocados no disco rígido, sem a autorização do administrador ou usuário, é considerado um *malware*, incluindo vírus, *trojans*, *worms*, *rootkits* e outros arquivos maliciosos.

Man-in-the-Middle-Atack – ocorre quando um computador intercepta conexões de dois outros.

Password-based Attacks – ataque gerado por programas criados no intuito de tentar senhas repetidas vezes em curtos intervalos de tempo, criando instabilidades na verificação do logon.

Phishing – são mensagens de e-mail criadas com interfaces e nomes que fazem referência a empresas famosas e conhecidas, onde são colocados links disfarçados que, se clicados, dão acesso a arquivos maliciosos.

Ransomware – é um tipo de *malware* que restringe o acesso ao sistema infectado e cobra um "resgate" para que tal acesso possa ser reestabelecido.

Rootkit – tipo de *malware* que se esconde nas bases do sistema operacional, em locais que não podem ser encontradas por antivírus comuns. São utilizados para interceptar solicitações do sistema operacional e alterar os resultados.

Scareware – *malwares* que mostram informações do tipo: “Você está infectado, clique aqui para limpar sua máquina”.

Spyware – são *malwares* instalados sem o consentimento dos usuários e utilizados para capturar informações de utilização e navegação.

Trojan – são *malwares* baixados pelo usuário sem que ele saiba e que escondem funcionalidades maliciosas capazes de alterar o sistema computacional para permitir ataques posteriores.

Vírus – são arquivos maliciosos anexos a outros arquivos.

Worm – funcionam de maneira similar aos vírus, mas não precisam de arquivos hospedeiros, podendo replicar-se automaticamente.

FABIO TORRES & ASSOCIADOS

Características gerais das Apólices

Conforme anteriormente exposto, Apólices de Riscos Cibernéticos têm coberturas de "primeira parte" e de "terceira parte". No mercado internacional, não é incomum que existam modelos de Apólices prevendo que cada uma dessas coberturas estará sujeita a um *triggering* distinto do outro, por exemplo, à base de "Descoberta" para as coberturas de "primeira parte", e de "Reclamação" para as coberturas de "terceira parte". No Brasil, porém, não se adotam *triggerings* distintos, e assim é que, em regra, as Apólices de Riscos Cibernéticos são em regra à base de Reclamações com Notificação, o que se justifica ante a dificuldade de se identificar a data em que ocorreu a violação do sistema de rede computacional e a quebra da privacidade do terceiro.

Com efeito, não é incomum que a violação e a quebra perdurem por anos a fio ou só sejam descobertas tempos após a sua concretização, de tal modo que, fossem as Apólices à base de Ocorrências, daí poderiam advir discussões e litígios infindáveis entre Segurados e Seguradoras, e destas entre si, acerca de qual Apólice daria cobertura para o ato danoso e a (s) Reclamação (ões) de terceiros.

Logo, o mais comum é que a Apólice aplicável seja aquela em vigor quando da apresentação da primeira Reclamação ao Segurado, Apólice, esta, a qual também se aplicará a todas as Reclamações conexas à primeira. Ademais, a Apólice permite ao Segurado, durante o período de vigência, notificar à Seguradora a ocorrência de um fato ou circunstância que, com base em um juízo de razoabilidade, seja apto a ensejar a apresentação de futuras Reclamações (a "expectativa"). Alguns clausulados autorizam a notificação de uma "expectativa" também durante o *extended reporting period* (que, no Brasil, abrange o prazo complementar, de contratação compulsória e sem adição de prêmio, e o suplementar, de contratação facultativa e sujeita ao pagamento de um prêmio adicional), porém condicionam que o fato ou circunstância descoberto e notificado durante o *ERP* tenha ocorrido durante o período de vigência.

Por sua vez, o fato ou circunstância notificado, normalmente, é o próprio ataque ou evento cibernético descoberto pelo Segurado, conforme definido na "Cláusula de Riscos Cobertos". Uma vez que o Segurado tenha tomado ciência de sua ocorrência e notifique formalmente à Seguradora, a notificação assim efetuada produzirá como efeito – atendidos os requisitos constantes na "Cláusula de Notificação" correspondente – a efetivação das coberturas de "primeira parte" porventura contratadas e, no tocante à cobertura de "terceira parte", a vinculação da Apólice em vigor às futuras Reclamações decorrentes do fato ou circunstância notificado. Contudo, diferentemente de outras Apólices tradicionais à base de Reclamações em que a notificação de uma "expectativa" não gera maior trabalho operativo e a Seguradora limita-se a fazer (ou se recusar a fazê-lo, se for o caso) o seu

registro, aqui a notificação serve à maneira de um autêntico aviso de sinistro em relação às coberturas de "primeira parte" e é um passo crucial no procedimento de regulação do sinistro, deflagrando a adoção de medidas emergenciais que visam à apuração das causas e extensão dos danos e à mitigação dos prejuízos.

A propósito da notificação/aviso, em poucos produtos o tempo de reação demandado aos Departamentos de Sinistros é tão importante como nos Seguros de Riscos Cibernéticos, e, justamente por isso, ocorre de as Apólices preverem um "gestor de sinistros" ou "de resposta a quebras ou atos de violação", a quem caberá coordenar os esforços dos profissionais envolvidos e que poderá ser contatado em regime integral (7d-24h) no caso de um incidente. Do mesmo modo, profissionais como *breach counsels* e *forensics experts* costumam ser selecionados por antecipação, com remuneração pré-definida, e indicados no "plano de resposta a incidentes" elaborado contemporaneamente à contratação do seguro. Isto evita que, em um estágio normalmente tenso como é o que se segue à descoberta de uma violação, Segurados e Seguradoras desperdicem seu tempo ou desgastem seu relacionamento com solicitações de documentos e análises de nomes e propostas de honorários.

No mercado internacional, as Apólices de Riscos Cibernéticos fixam prazos estritos para a notificação/aviso à Seguradora, cujo descumprimento gera a perda do direito à cobertura (nos Estados norte-americanos, não se costuma exigir a comprovação do prejuízo para a aplicação da sanção de perda de direitos); no Brasil, porém, o art. 39 da Circular SUSEP 256/2004 veda às Seguradora estabelecer um prazo decadencial para o aviso de sinistro. Isto não significa que a Seguradora não possa negar cobertura em razão de uma comunicação tardia, mas lhe impõe, por aplicação do princípio da boa-fé, o ônus de comprovar que da demora do Segurado em proceder ao aviso decorreu um prejuízo material concreto.

Sendo uma Apólice à base de Reclamações, a Seguradora poderá admitir um período de retroatividade da cobertura – que, em renovações sucessivas, será a data da primeira contratação à base de Reclamações. Neste caso, as Reclamações decorrentes de ataques ou eventos cibernéticos ocorridos anteriormente ao momento da contratação terão cobertura na Apólice, desde que: (i) tal ocorrência tenha se dado após a data limite de retroatividade e (ii) quando da contratação, tais ataques ou eventos fossem desconhecidos pelo Segurado. Considerando-se a possibilidade de que tais eventos permaneçam latentes por período relativamente extenso, a Seguradora deve ter cautela ao admitir o período de retroatividade.

Exclusões mais presentes

Abaixo estão várias exclusões importantes a se ter em consideração quando se examina uma Apólice de Riscos Cibernéticos. Uma vez mais, deve-se ter em conta que não há uma uniformidade na redação das condições contratuais, de modo que é possível que algumas Seguradoras cubram alguns dos riscos a seguir, quer em suas Apólices originais, quer por meio de *buy-back*:

Aparelhos Eletrônicos Portáteis – Se o dispositivo eletrônico que leva a uma violação de segurança ou privacidade for portátil (por exemplo, um *laptop* ou um *smartphone*), algumas Apólices podem excluir cobertura para os danos daí decorrentes.

Atos Dolosos ou Intencionais de Representantes Legais do Segurado– Ressalva-se que o art. 22, parágrafo único, da Circular SUSEP 256/2004 veda tal exclusão quando se tratar de ato desonesto praticado por empregado.

Danos a clientes corporativos - Algumas vezes a cobertura de "terceira parte" da Apólice de Riscos Cibernéticos estender-se-á apenas consumidores que sejam pessoas físicas, e não para terceiros que sejam clientes corporativos.

Atos praticados ou Reclamações apresentadas fora dos limites territoriais previstos na Especificação da Apólice – autoexplicativo.

Guerra/Terrorismo/Eventos da Natureza ou de Força Maior – As Apólices podem prever que ataques cibernéticos praticados no contexto de uma guerra militar ou civil, declarada ou não, bem como com propósitos políticos (como o cyberterrorismo), estão excluídos da cobertura securitária. O mesmo ocorre se a perda, dano ou a destruição de dado resultar de um fenômeno natural, como um terremoto ou furacão.

Negligência na Segurança do Sistema de Computação – Algumas Apólices podem excluir os danos resultantes da negligência do Segurado em adotar medidas de segurança preventivas exigidas à maneira de *warranties*, como, por exemplo, a observância de normas de procedimentos para autenticação de usuários, *firewalls*, atualização com determinada periodicidade mínima do *software* de antivírus e detecção de intrusão, criptografia de dados, programas de manutenção e testes de vulnerabilidade, além de sistemas eletrônicos que forneçam controle de acesso por meio do uso de senhas, identificação biométrica ou similar de usuários autorizados. É importante assinalar que tais exigências deverão ser feitas na contratação do seguro e que, em consonância à nossa jurisprudência, somente darão ensejo à negativa de cobertura se a Seguradora estiver apta a demonstrar a existência de um nexo de causalidade entre a medida não adotada e o dano decorrente.

Dados sob a Guarda, Custódia ou Controle de Terceiros – Muitas Apólices excluem cobertura para a responsabilidade do Segurado pela perda, danos ou destruição de dados confiados à guarda ou custódia de terceiros.

Conclusão

FABIO TORRES & ASSOCIADOS

Riscos cibernéticos são uma realidade dos nossos tempos e, não importa quanto seja gasto com prevenção, mais eventos danosos (ou potencialmente danosos) acontecem a cada dia. É improvável que exista uma só empresa que possa se afirmar imune à violação da sua segurança e à quebra da privacidade de dados. Por sua vez, dado que o uso intensivo de sistemas informatizados aumenta exponencialmente o alcance dos danos, espera-se o pagamento de somas ainda mais vultosas a cada violação.

Além disto, os procedimentos de *compliance* e resposta a incidentes podem ser tornar ainda mais complexos, haja vista que o Projeto de Lei nº 330/2013 – que trata da privacidade de dados – avança no Senado Federal e, após passar por Comissões diversas, chegou em julho de 2016 à Comissão de Assuntos Econômicos, penúltima etapa antes da sua deliberação no plenário daquela Casa. Sua tramitação tem-se mostrado rápida e, em paralelo a ele, tramita outro projeto, originário do Poder Executivo, no âmbito da Câmara dos Deputados. Em contato com assessores parlamentares, fomos informamos de que a expectativa é uma aprovação relativamente célere no Senado Federal, com o que, quando do envio à Câmara dos Deputados, ocorreria a apensação de ambos os projetos sobre o tema. Não há dúvida de que a aprovação do Projeto – qualquer que seja a sua formatação final – servirá de estímulo ao desenvolvimento dos Seguros de Cyber no Brasil, assim como o foi nos EUA.

Por sua vez, aos benefícios advindos da adoção de um mecanismo de transferência de riscos, somem-se as vantagens de procedimentos de subscrição de riscos que poderão ajudar as empresas a identificar lacunas de segurança cibernética e oportunidades de melhoria em seus sistemas. O Seguro de Riscos Cibernéticos contribui para a criação de práticas mais seguras de *cyber security*, já que na subscrição a empresa deverá submeter seus controles administrativos, técnicos e físicos ao escrutínio da Seguradora.

Além de proporcionar a função de transferência de riscos, as Apólices de Riscos Cibernéticos trazem um valor adicional aos Segurados, porquanto, em um momento particularmente difícil da atividade organizacional, conferem-lhes ferramentas valiosas de mitigação de danos e assistência à resposta que podem ser essenciais especialmente para as pequenas empresas (as quais normalmente não têm experiência ou mão-de-obra adequada), quando confrontadas com danos potenciais de grande porte à sua imagem e reputação.

Por tudo isto, estamos certos de que o Seguro de Riscos Cibernéticos veio para ficar; o desafio, para nós, é entendê-lo e aplicá-lo.

*

* *