Hackers Atacam Novamente! Análise de Invasões no Setor de Saúde à Luz do Seguro de Responsabilidade Civil por Riscos Cibernéticos e Proteção de Dados

Felipe Goulart Bastos*

Úrsula de Ávila Goulart Bastos**

Introdução. Ataques Cibernéticos no Setor de Saúde

"Hackers invadem sistema do Hospital do Câncer de Barretos e pedem resgate"[1]

"Ataque de hackers ao Hospital do Câncer de Barretos prejudica atendimento a pacientes"[2]

Há poucos dias, aos 27 de junho, hackers invadiram o sistema do Hospital do Câncer de Barretos, bloquearam os acessos a dados de pacientes e exigiram um resgate de US$ 300,00 em *bitcoins* por computador, para liberar o sistema. A ação afetou diversas unidades do Hospital em outras cidades e Estados.

Cerca de um mês antes, um ciberataque fez mais de 200 mil vítimas, em pelo menos 150 países, num alcance global sem precedentes. O ataque *hacker* atingiu quase 20% do sistema de saúde do Reino Unido. Dados de pacientes foram encriptados pelos invasores e se tornaram inacessíveis para os agentes públicos. Por meio dos computadores invadidos, os hackers cobraram o pagamento de US$ 600,00 em
bitcoins
para recuperar os dados encriptados.

Embora ainda relativamente pouco conhecidos no país, ataques cibernéticos a hospitais, operadoras de planos de saúde e sistemas públicos de saúde têm se tornado uma prática cada vez mais frequente. Relatório especializado elaborado pela IBM demonstra que a indústria da saúde foi o principal alvo de hackers em todo o mundo em 2015, a frente de segmentos até então tidos como vítimas mais óbvias, como setores industriais e empresas do ramo financeiros, como bancos de varejo e de investimentos.[3] Mais de 100 milhões de registros relacionados ao setor de saúde foram violados por ataques cibernéticos em 2015, segundo o relatório.

A recente ofensiva sobre o Hospital do Câncer de Barretos, São Paulo, demonstra que o Brasil não está imune a este tipo de ação criminosa.

O crescimento exponencial do risco cibernético é um fenômeno inexorável. Assim, é natural que surjam dúvidas a respeito de como gerenciá-lo. Dentre as opções de gerenciamento, o seguro aparece como uma possível alternativa aos astronômicos prejuízos financeiros decorrente dessas ações criminosas.

Há uma pluralidade infindável de riscos cibernéticos, de sorte que seria impossível dissecá-los nos limitados confins desse artigo. Portanto, o nosso propósito é, a partir de uma hipótese similar ao ataque ao Hospital de Barretos (SP), delinear brevemente quais desafios as vítimas desses tipos de invasões no setor de saúde enfrentam e analisar até que ponto os riscos dele decorrentes podem ter suas repercussões financeiras gerenciadas por meio de seguros no Brasil.

Gerenciando a Crise

No dia do ataque cibernético ao Hospital do Câncer de Barretos, notícias dão conta que aproximadamente 3.000 consultas e exames foram cancelados, e 350 pacientes deixaram de realizar tratamentos de radioterapia.[4]

Numa tal situação de crise, diversas providências assistenciais imediatas se fazem imprescindíveis. Elas incluem identificar e, em seguida, reagendar todas os milhares de exames, consultas, procedimentos e tratamentos (em conjunto, as “providências médicas”) cancelados em razão do bloqueio de acesso aos registros dos pacientes.

Nesse trabalho, a administração hospitalar se depara com o problema de acomodar conflitos entre as providências médicas diretamente postergadas com o agendamento de outros pacientes, inclusive de pacientes novos.

Na dimensão tempo, agilidade máxima é absolutamente indispensável no serviço de implantação de servidor substituto ou recuperação do original. Além disso, deve-se procurar resgatar de pronto o arquivo de *backup* – espera-se que haja um! –, a fim de se restaurar os dados perdidos dos pacientes. Porém, há que se atentar para o fato de que raramente *backups* serão completos – eles não incluem as informações entre a data de realização do *backup* e a data ou hora do ataque si.

No total, foram necessários 6 dias para o Hospital do Câncer de Barretos anunciar publicamente a normalização dos atendimentos em todo o país.[5]

Perdas decorrentes do *Cyberattack*

No interregno entre o ataque a normalização das operações hospitalares, perdas financeiras se avolumam. Despesas geralmente elevadas incluem aquelas necessárias para custear serviços emergenciais de TI para a reconstrução da rede, restabelecimento do servidor e recuperação de dados dos pacientes.

A par disso, supõe-se que os funcionários do hospital tiveram que trabalhar além da jornada habitual no trabalho de reagendamento das providências médicas, ocasionando custos trabalhistas com horas extras e até mesmo com a contratação de prestadores de serviços. Isso sem mencionar os prejuízos decorrentes das perdas de receita do hospital em virtude dos cancelamentos dos exames, consultas, tratamentos etc. É de se cogitar, outrossim, que pacientes em situações críticas ou emergenciais quando nas primeiras horas que sucederam ao incidente podem ter tido que ser removidos para outras unidades hospitalares, gerando, assim, por sua vez, novas perdas para o Hospital do Câncer de Barretos.

Outras perdas têm natureza reputacional – a vulnerabilidade no sistema de segurança exposta a partir de uma invasão hacker pode minar a confiança junto a pelo menos uma parcela de seus usuários.

No incidente envolvendo o Hospital do Câncer de Barretos, as informações públicas disponibilizadas a respeito do episódio sugerem que os dados de pacientes bloqueados não chegaram a ter o seu conteúdo acessado pelos invasores. O vazamento de informações sigilosas e dados pessoais de pacientes exporia o hospital a milhares de demandas judiciais em busca de reparação material e/ou moral, elevando as perdas a patamares estratosféricos.

Notícias apontam que não houve pagamento de resgate – o que constituiria, per se, uma espécie de perda também – somente na unidade de Barretos do Hospital havia quase mil computadores, fazendo o resgate largar, numa conta muito rápida, de praticamente R$ 1 milhão (o total, se atendidos os pedidos dos hackers, seria muito mais elevado).

O Mercado de Seguros para Riscos Cibernéticos

No mercado externo, existe uma multiplicidade de produtos sobre riscos cibernéticos. São produtos não comoditizados e que de tão distintos por vezes torna-se difícil para o corretor ou, principalmente, o segurado compará-los.

A subscrição dos seguros cibernéticos apresenta profundos desafios técnicos. Enquanto ramos tradicionais dispõem de dados históricos bem consolidados e muito específicos sobre padrões de *(a)* perdas; *(b)* indenizações reclamadas; *(c)* custos de defesa; *(d)* tempo de regulação de sinistros; e *(e)* indenizações pagas, as ocorrências de *cyberattacks* são algo erráticas, carecendo de consistência quanto a tais aspectos fundamentais.

Há uma diversidade colossal de formas de ataques. Novas modalidades de incidentes surgem a cada dia, tornando impossível se produzir uma tipologia exaustiva dessas ações. Uma das principais dificuldades associadas ao desenvolvimento de seguros contra riscos cibernéticos reside precisamente na falta de informações completas, específicas e homogêneas sobre tais eventos, sua frequência e severidade. A imperfeição da agregação de informações afeta a capacidade dos atuários de desenvolver produtos de seguros mais consistentes e robustos, ocasionando certos riscos nas atividades de subscrição e precificação dessas apólices.

O mercado de seguros para riscos cibernéticos ainda é bastante tímido no Brasil. São poucas as seguradoras que dispõem de produtos aptos à contratação: AIG, XL e muito recentemente a Zurich. Tais produtos são quase reproduções traduzidas para o português, com poucas adaptações, de clausulados mais experimentados em mercados maduros. Contudo, a rebote dos ataques cibernéticos mais recentes e da escalada na demanda, seguradoras como Chubb, Argo, Allianz, Generali - e até mesmo a fintech de seguros Thinkseg, por meio de parceria - já declararam o interesse em se lançar nesse mercado.

As Apólices de Riscos Cibernéticos no Brasil. Separando o Joio do Trigo: Quais Riscos Estão Garantidos e Quais Estão Descobertos

No Brasil, o “Seguro de Responsabilidade Cibernética e Proteção de Dados”[6] e seus congêneres foram desenvolvidos para proteger o segurado contra as exposições cibernéticas multidisciplinares. Dentre as proteções possíveis incluem-se as de segurança na rede, mídia

on-line
, propriedade intelectual e privacidade, mitigando os riscos de proteção, gestão e manuseio de dados pessoais, tais como registros médicos e informações financeiras e cartões de crédito, e as consequências das perdas de informações corporativas.

Embora esse seguro seja classificado como de "Responsabilidade Civil"[7] – isto é, aquele que visa reparar os prejuízos sofridos pelo segurado em virtude de uma reclamação de terceiro [8]
-, as apólices disponíveis no mercado oferecem também coberturas
first party
– ou seja, para os danos sofridos pelo próprio segurado [9]
(custas, despesas e perdas e danos ao seu patrimônio). Normalmente, as garantias se referem a

i) Interrupção da rede (cobertura/extensão adicional): perdas ou atrasos na prestação de serviços e/ou vendas e despesas extraordinárias, inclusive operacionais, relativas a ataques cibernéticos que ocasionem o comprometimento de sua rede, bem como os lucros cessantes daí decorrentes, reais e mensuráveis;

ii) *Ativos intangíveis ou reposição por perda de dados* (cobertura/extensão adicional): gastos para que seja determinado se os dados eletrônicos danificados em virtude de um ataque malicioso podem ou não ser restaurados, restabelecidos ou recriados, e para fazê-los, quando possível;

iii) *Notificação e despesas por crise de gestão devido à violação de informação pessoal* (cobert ura/extensão adicional): garante o pagamento de honorários, custas e despesas razoavelmente incorridos pelo segurado na contratação de profissionais especializados visando à notificação sobre a violação de informação pessoal ou de segurança de dados aos clientes/terceiros;

iv) *Extorsão na internet* (cobertura/extensão adicional): pagamento de prejuízos decorrentes de extorsão por terceiros que tenham cometido ou que ameacem cometer o comprometimento da rede ou violação de publicações;

v) *Restituição de Imagem do Segurado e Pessoal* (em geral, por cobertura/extensão adicional): custos e despesas referentes a honorários incorridos pelo segurado pata obter aconselhamento de um consultor de relações públicas e mitigar os danos à reputação em consequência de um evento coberto pela apólice;

vi) *Custos de Defesa* (em geral, como cobertura básica): honorários advocatícios e custas judiciais incorridos exclusivamente da defesa ou recurso de um procedimento civil, regulatório, administrativo ou criminal [10];

vii) *Despesas de salvamento ou Despesas de mitigação* (em geral, por cobertura/extensão adicional): pagamentos realizados, razoáveis e necessários, ou custos incorridos em conexão com a violação de dados pessoais e corporativos visando evitar e/ou minorar uma reclamação de terceiro, ou reduzir potenciais perdas ou compensações passíveis de amparo, sujeitos a limites específicos.

Abra-se um parêntese para assinalar que, no caso do Hospital de Câncer de Barretos, segundo as informações públicas divulgadas, quase todas as coberturas acima teriam utilidade, exceto pelas designadas nos itens (iii), eis que aparentemente não chegou a ocorrer violação propriamente dita de dados pessoais e informações confidenciais pelos hackers, apenas o bloqueio delas para o Hospital; e (vi), haja vista que não temos notícia ainda de reclamações formuladas por terceiros contra o Hospital, conquanto seja natural se esperar que ocorram investigações do incidente por parte de autoridades regulatórias e até policiais.

No âmbito dos danos causados a terceiros (*third party*), as seguradoras ofertam, em regra, as seguintes coberturas:

i) *Responsabilidade por Dados Pessoais e Corporativos*: garante o pagamento das perdas decorrentes da divulgação pública de dados privados e corporativos, real ou presumida, que resulte em uma reclamação contra o segurado. Por dados corporativos entendem-se quaisquer segredos de um terceiro (por exemplo: orçamentos, listas de clientes, planos de marketing etc), cuja divulgação seja vantajosa para um concorrente, ou qualquer informação que não esteja disponível ao público em geral, bem como informações profissionais confidenciais de um terceiro que estejam sob a custódia do segurado;

ii) *Responsabilidade pela Segurança de Dados*: garante o pagamento das perdas decorrentes de ato, erro ou omissão na segurança de dados que resulte em: a) contaminação de dados de terceiro por *software* não autorizado ou código malicioso (vírus); b) negação de acesso inadequada ou imprópria para o acesso aos dados pelo terceiro autorizado (negação do serviço); c) roubo de código de acesso nas instalações do segurado ou via sistema de computador; d) destruição, modificação, corrupção, dano e eliminação de dados armazenados em qualquer sistema de computador; e) Roubo físico de hardware do segurado por um terceiro; f) Divulgação de dados devido a uma violação de segurança de dados;

iii) *Responsabilidade por Empresas Terceirizadas*: violação de informação pessoal que resulte em uma reclamação contra uma empresa terceirizada pelo processamento ou coleta de dados pessoais em nome do segurado e pelos quais ele é responsável.

iv) *Responsabilidade por Conteúdo de Mídia* (cobertura/extensão adicional): responsabilidade civil associada à compilação, criação, publicação, impressão, difusão ou distribuição de qualquer conteúdo de mídia, digital ou digitalizado que resulte em uma infração de direitos autorais (*copyright*), plágio, pirataria, apropriação indevida e roubo de ideias, divulgação pública de fatos privados, dentre outros.

Quer-nos parecer que a estrutura do clausulado dessas apólices aqui no Brasil, que não é padronizada, seja de “riscos nomeados” (vale dizer, não é *all risks*) – ou seja, os riscos cobertos são apenas aqueles nominalmente definidos e hermeticamente delimitados, sendo que os riscos excluídos variam de seguradora para seguradora. Quanto a estes últimos, os mais comuns se referem a reclamações decorrentes de:

i) atos ilícitos e dolosos do segurado e seus representantes legais;

ii) danos corporais, estéticos, materiais e morais, estes últimos salvo se decorrerem de um fato coberto;

iii) qualquer responsabilidade ou obrigação contratual ou violação de qualquer contrato, inclusive penalidades contratuais, exceto com relação a violações e obrigações de

confidencialidade relativas a dados pessoais e corporativos vinculados a fatos geradores cobertos;

iv) guerra, terrorismo, tumultos, greves, rebelião, insurreição, confisco decorrentes de qualquer ato de autoridade civil ou militar, e eventos similares;

v) falha mecânica, elétrica, dos sistemas de telecomunicação ou de transmissão via satélite.

Todas as apólices de Riscos Cibernéticos disponíveis no Brasil são à base de Reclamações com Notificação. Essa modalidade nos parece adequada, tendo em vista que, muitas vezes, haverá dificuldade em se determinar o momento exato em que ocorreu o ato danoso ou o fato gerador – muitos riscos cibernéticos podem ser de latência prolongada (*e.g.*, ameaças de invasões; implantações de vírus com liberação tempos depois etc.). Assim é que há cobertura, também, para reclamações de terceiros com relação a fatos e circunstâncias ocorridos entre a data limite de retroatividade, inclusive, e o término da vigência da apólice, desde que tenham sido notificados pelo segurado durante a sua vigência.

Notas Finais

"*Cyber Attack risk is increasing rapidly and is likely to remain highly elevated in the short term, with high uncertainty in the pattern of future risk."* [11]

O que parecia digno das grandes tramas de ficção do cinema existe há um bom tempo no mundo real. O Brasil é também alvo de ofensivas e sofre com os efeitos dos ataques cibernéticos em massa recentemente ocorridos em todo o mundo. Órgãos do Judiciário e empresas de ramos diversos foram concretamente afetadas. As consequências são inexoráveis: vulnerabilidade em relação a dados pessoais e informações digitais, suscetibilidade a imensos prejuízos financeiros, com a consequente busca por soluções e programas de gestão de riscos corporativos para prevenir e/ou mitigar os danos daí decorrentes.

No setor de saúde, os riscos cibernéticos são bem mais sensíveis do que na maioria dos outros

segmentos. Eles decorrem, especialmente, de alguns importantes fatores: a quantidade significativa de informações com dados médicos confidenciais e identificação pessoal dos doentes, que são transmitidas e armazenadas no sistema; a crescente utilização de dispositivos móveis; a enorme dependência de serviços terceirizados; a complexa cadeia de responsabilidades devido à pluralidade de relações existentes; múltiplos pontos de acesso aos sistemas de rede; e a possibilidade, sob o ponto de vista ético, da criação de registros pessoais de saúde eletrônicos[12].

O caso do Hospital do Câncer de Barretos é emblemático e está fresco na memória. Além dos prejuízos financeiros diretos e os decorrentes de danos à imagem e reputação (certamente elevados), estão em jogo (*i.e.*, sob tutela), sobretudo, a saúde, a intimidade e até a vida dos pacientes. Consultas e exames cancelados, incluindo tratamentos de radioterapia, atendimento diário a milhares de pacientes interrompido e riscos de perda/divulgação de dados e prontuários médicos digitais: estes foram os prejuízos até então divulgados publicamente.

Nesse contexto, tanto o setor público quanto o privado no Brasil precisarão passar por um longo, porém inevitável, processo de conscientização sobre suas exposições a riscos cibernéticos. Nesse ambiente, torna-se altamente recomendável a adoção de programas e medidas de prevenção/mitigação contra tais riscos[13], especialmente pelos muitos entes – decerto a maioria deles – que não possuem experiência e estrutura adequadas. Essa consciência tanto deverá ser maior quanto mais expostos forem os segmentos a responsabilizações civis. É o caso do setor médico-hospitalar, por conta dos bens da vida tutelados e de dependerem, para suas atividades, da coleta e manejo de dados pessoais e informações confidenciais. Além disso, diversamente de empresas do setor financeiro (bancos, administradoras de cartões de crédito), hospitais costumam ser vistos como historicamente menos preparados para a proteção contra fraudes e violações de dados – logo, mais vulneráveis a ataques. [14]

Ainda que não existam ainda no Brasil dados estatísticos e empíricos abundantes sobre o comportamento do nosso mercado no setor[15], não podemos olvidar dos benefícios e vantagens que as garantias e coberturas *first party* e *third party* das Apólices de Riscos Cibernéticos oferecem para enfrentar as consequências financeiras desses eventos. Que esse segmento se expanda e se desenvolva, pois, lamentavelmente, há absoluto consenso de que a tendência dos riscos cibernéticos é de grande escalada nos próximos anos.
[16]

* Sócio de Veirano Advogados; Mestre em Direito (LL.M., com honras acadêmicas) pela University of Virginia School of Law, EUA; Pós-graduado (MBA) em Direito Securitário pela Escola Superior Nacional de Seguros – Funenseg; Bacharel em Direito pela UERJ. ** Sócia de Gondim Advogados; Mestre em Direito Civil pela UERJ; Pós-graduada pela EMERJ; Professora de Direito Securitário na PUC-Rio; Bacharel em Direito pela Universidade Cândido Mendes.

[1] http://www1.folha.uol.com.br/cotidiano/2017/06/1896638-hackers-invadem-sistema-do-hospital-de-cancer-de-barretos-e-pedem-resgate.shtml

[2] http://noticias.r7.com/sp-no-ar/videos/-ataque-de-hackers-ao-hospital-do-cancer-de-barretos-prejudica-atendimento-a-pacientes-29062017

[3] "Top 5 Industries At Risk Of Cyber-Attacks", https://www.forbes.com/sites/stevemorgan/2016/05/13/list-of-the-5-most-cyber-attacked-industries/#35273e19715e

[4] http://g1.globo.com/sp/ribeirao-preto-franca/noticia/ataque-de-hackers-suspende-3-mil-consultas-e-exames-nas-unidades-do-hospital-de-cancer-de-barretos-sp.ghtml

[5] http://www.correiodolago.com.br/noticia/seis-dias-apos-ataque-cibernetico-hospital-de-cancer-de-barretos-tem-atendimentos-normalizados-em-todo-o-pais/55231/

[6] Ou “Seguro de Proteção de Dados e Responsabilidade Cibernética”. A Zurich lançou o produto recentemente com o nome “Proteção Digital”.

[7] A propósito desta classificação, consultamos a Circular SUSEP Nº 535/2016. Notamos que os produtos registrados pelas três seguradoras que operam com “apólices de cyber risks” foram classificados em ramos diversos. A AIG possui dois registros: um principal, classificado no ramo “RC Geral” (dentro do Grupo “Responsabilidades”) – mesma classificação do produto da Zurich - e outro secundário, classificado em “lucros cessantes”, que está enquadrado no Grupo “Patrimonial”. A XL, por sua vez, teve seu registro enquadrado no ramo “RC Profissional” (também dentro do Grupo “Responsabilidades”).

[8] O “Objetivo do Seguro” nas três apólices disponíveis no mercado é definido como sendo:

i) “o pagamento das Perdas devido a Terceiros pelo Segurado decorrente de uma Reclamação”. (AIG);

ii) “a INDENIZAÇÃO AO SEGURADO, relativa a reparações por PREJUÍZOS consequentes de danos causados a TERCEIROS”. (XL)

iii) “Mediante o pagamento do Prêmio, sujeito à Franquia e até o Limite Máximo de Garantia, o

Limite Agregado e o Limite Máximo de Indenização correspondente, a Seguradora garante ao Segurado o reembolso dos Danos que este for obrigado a pagar em decorrência da sua responsabilidade civil definida no âmbito da (s) Reclamação(ões) apresentada (s) por um ou mais Terceiros contra tal Segurado, coberta (s) pela Apólice, na forma destas Condições Gerais e das Condições Especiais aplicáveis a cada cobertura contratada, desde que atendidas as disposições da Apólice. (Zurich)

[9] Em
https://www.editoraroncarati.com.br/v2/phocadownload/cyber_risks_setembro_2016.pdf
Fábio Torres e Associados, classificam as coberturas disponíveis em coberturas de “primeira parte”, ou seja, destinadas as “danos diretos” e coberturas de “terceira parte”, isto é, “danos indiretos” ou “de responsabilidade”.

[11] Cambridge Global Risk Index 2017 (
https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/cambridgeglobalriskindex2017.pdf
).

[12] Conforme RESOLUÇÃO CFM Nº 1.821/07, que aprova as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel e a troca de informação identificada em saúde.

[13] Programas, medidas e controles estes que são submetidos/avaliados pela Seguradora nos procedimentos de subscrição da apólice de Riscos Cibernéticos, o que acaba levando as empresas a criarem práticas mais seguras e eficazes de segurança cibernética.

[14] “Why Hackers are After the Healthcare Industry” (
https://www.tripwire.com/state-of-security/security-data-protection/cyber-security/why-anthem-why-now/
)

[15] A primeira apólice de Riscos Cibernéticos comercializada no Brasil se deu no início de 2014, pela XL, seguida pela AIG, em 2015 e, muito recentemente (junho de 2017), pela Zurich.

[16] “Risk of major economic shocks from cyber attacks is increasing, and is elevated by 20% above baseline as we face a period of increased risk.” Cambridge Global Risk Index 2017 (
https://www.jbs.cam.ac.uk/fileadmin/user_upload/research/centres/risk/downloads/cambridgeglobalriskindex2017.pdf
)

(10.07.2017)