Ciber-risco
e Seguro

Coleção
KEEP IT
SIMPLE
MDS

Geoff Kinsella

MDS
Publications

Ciber-risco
e Seguro

Coleção
KEEP IT
SIMPLE
MDS

Geoff Kinsella

MDS
Publications

Título do Livro: Ciber-risco e Seguro

Autor: Geoff Kinsella

Coleção: Keep It Simple

Editor: MDS Group

Tiragem: 300 exemplares

Data de impressão: Agosto 2022

Depósito Legal: 503643/22

ISBN: 978-989-54810-5-7

Impressão: Lidergraf, Sustainable Printing

Índice

II. O que é coberto por uma apólice de seguro de ciber-risco?

Com a expansão do cenário de ameaças digitais em que as empresas operam, é de grande importância avaliar e mitigar o ciber-risco e proteger as atividades contra este risco. O ciber-seguro devia fazer parte integral de qualquer abordagem de gestão de risco de segurança cibernética. O apoio adicional prestado antes e depois do prejuízo por muitas seguradoras de ciber-risco será uma vantagem significativa para qualquer organização.

Geoff Kinsella, FCII [*Fellowship of the Chartered Insurance Institute (FCII)*], MBA, consultor de seguros que trabalha na área do ciber-seguro há mais de 10 anos, acredita que as principais razões de o ciber-seguro ainda não ser comummente adquirido assentam na falta de conhecimento e de valorização da cobertura e vantagens associadas a esta classe emergente.

Neste livro, exploramos a evolução do ciber-seguro, explicamos a cobertura e as suas vantagens e oferecemos algumas perspetivas sobre considerações na gestão de ciber-risco nas empresas. Tentaremos igualmente destacar alguns dos mercados que lideram este espaço e a forma como o mercado pode evoluir no futuro.

“ É comum ouvir os peritos em segurança cibernética dizer que “não se trata somente de uma questão de tempo até alguém atacar os nossos sistemas de segurança. Provavelmente já foram atacados!”.

Portanto, quando as coisas correm mal, é importante ter implementado um programa de gestão de risco para ajudar a empresa a mitigar o impacto de um sinistro cibernético.

O seguro de risco cibernético deve fazer parte da resposta de gestão de risco das empresas. ”

I. Risco cibernético - uma ameaça crescente

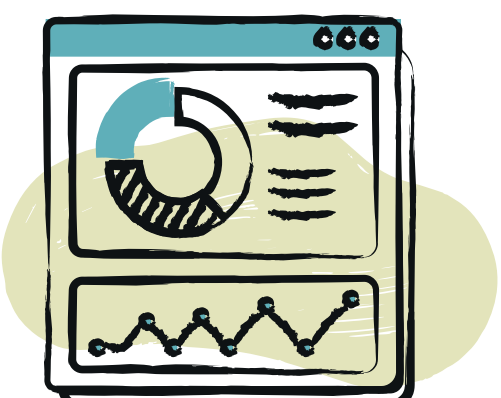
Acha que o progresso tecnológico está a levar a um aumento da necessidade de proteção contra o risco cibernético?

Sem dúvida. Embora pareça um chavão, vivemos inquestionavelmente num mundo digital interdependente. Quando a Internet surgiu na esfera pública, estávamos em meados da década de 1990. A maior parte das pessoas, mesmo eu, não anteviam o impacto notável que viria a ter. Desde a forma como adquirimos bens e serviços à forma como comunicamos entre nós, a tecnologia, de uma forma ou de outra, infiltrou-se em todos os aspetos da nossa vida. O ritmo da mudança é assustador.

A "Internet das Coisas" ainda veio adicionar outra camada de interligação que permeia muitos dos produtos que temos. Seja o carro na nossa garagem, o contador inteligente em casa ou os eletrodomésticos na cozinha, a tecnologia permite-nos agora — mas também a terceiros — monitorizar remotamente e

simplificar a nossa rotina diária.

Já nos acostumámos todos ao facto de que as entidades com quem interagimos online recolhem os nossos dados pessoais. No passado recente, poderíamos imaginar esta cedência tão pronta da nossa informação a pessoas que nos são totalmente desconhecidas? Desde a data de nascimento aos dados da carta de condução; do nome de solteira da nossa



mãe ao número de conta bancária: andamos todos alegremente a preencher formulários na Internet que dão ao destinatário as chaves da nossa vida. Os dados são a nova "moeda" e o volume de dados recolhido é inaudito. Li recentemente que foram gerados mais dados nos últimos dois anos do que em toda a história humana anterior!

Este apetite por dados não vai desacelerar. Já nem se pode ir dar um passeio sem querer registar o número de passos que se deu! No motor de busca Google, fazemos cerca de 95.000 pesquisas por segundo. No YouTube, aparecem 500 horas de vídeo a cada minuto que passa e, nesse mesmo minuto, os utilizadores mandam 8 mil milhões de mensagens pelo Facebook! Espantoso.

No motor de busca Google, fazemos cerca de 95.000 pesquisas por segundo

Quanto mais nos fiarmos na tecnologia para dar forma às nossas vidas, mais crescerá a procura de proteção contra o risco cibernético.

A utilização da tecnologia também tem impacto no mundo empresarial?

A tecnologia está claramente a transformar a forma de fazer negócio. Usamo-la para comprar, vender, conceber e desenhar, transportar, fazer reuniões, vigiar, avaliar e muito mais. Cresce a dependência dos sistemas que usamos, quer se trate de tecnologias informativas ou operacionais. Tal como sucede nas nossas vidas privadas, as empresas começaram a interagir digitalmente com os seus fornecedores, partilhando informação privilegiada e, muitas vezes, permitindo-lhes o acesso aos seus sistemas. As empresas guardam uma enorme quantidade de Dados Pessoais Identificáveis (DPI) sobre os seus clientes, o que as ajuda a criar a experiência do cliente. Tal como fez com a nossa vertente pessoal, a tecnologia infiltrou-se em muitos dos processos e equipamentos utilizados na indústria para permitir a monitorização e controlo remotos. Com o acesso remoto vêm perigos inerentes.

Cresce a dependência dos sistemas que usamos, quer se trate de tecnologias informativas ou operacionais

O potencial de aumento do rendimento líquido das empresas, redução dos custos e aumento das margens operacionais pela adoção de enorme quantidade de dados gerados (*Big Data*) estão, sem dúvida, a motivar uma maior utilização de tecnologia. Num estudo da Accenture de 2014, intitulado "Big Success with Big Data" ("Grande Sucesso com Big Data"), constatou-se que 79% dos executivos na altura acreditavam que a não adoção do Big Data acabaria por levar à insolvência das empresas. No passado, a transformação digital era um desejo. Agora, é um imperativo de sobrevivência. Se olharmos para a velocidade com que as organizações tiveram de transferir a maior parte da sua força laboral para o trabalho remoto devido à pandemia, veremos que tal não teria sido possível sem a revolução digital que já estava em curso. Esta revolução vai continuar a definir o nosso mundo.

As empresas gastam somas avultadas na segurança e na estabilidade dos seus sistemas. Se a tecnologia falhar, seja por que motivo for, poderá haver impactos severos na subsistência dos trabalhadores e na rentabilidade e longevidade das empresas.

Torna-se cada vez mais importante para as empresas proteger-se de eventuais adversidades ligadas à àrea cibernética.

O que acontece quando as coisas correm mal?

É comum ouvir os peritos em segurança cibernética dizer que “não se trata somente de uma questão de tempo até alguém atacar os nossos sistemas de segurança. Provavelmente já foram atacados!”.

Todos lemos notícias de primeira página sobre grandes empresas que foram gravemente afetadas pelas consequências de falhas nos seus sistemas. Essas empresas têm frequentemente dificuldade em recuperar, tanto do ponto de vista financeiro como do da reputação. Mas, por cada notícia que chega às páginas dos jornais, há muitas outras empresas que sofrem prejuízos devidos a acontecimentos adversos no domínio cibernético que não são denunciados. Também é de interesse notar que a grande maioria dos sinistros em ciber-segurança afetam Pequenas e Médias Empresas (PME). Um estudo recente da NetDiligence (prestador de serviços de prontidão e resposta contra ciber-risco) apontou que 98% de todos os sinistros ocorridos de 2015 a 2019 afetaram PMEs. 77% dessas empresas declarava rendimentos inferiores a 300 milhões de dólares.

Portanto, quando as coisas correm mal, é importante ter implementado um programa de gestão de risco para ajudar a empresa a mitigar o impacto de um sinistro cibernético. O seguro de risco cibernético deve fazer parte da resposta de gestão de risco das empresas.

Então, por que motivo o ciber-seguro tem demorado tanto tempo a desenvolver-se?

Existem muitas razões, mas em minha opinião uma das principais é a falta de conhecimento sobre o produto e o que ele garante. O número de empresas a adquiri-lo aumentaria se, por exemplo, tivessem mais consciência do âmbito da cobertura que lhes é dada por uma apólice de seguro contra risco cibernético?

De igual modo, muitos compradores acham que o ciber-seguro é uma linha de negócio muito recente que ainda tem de dar provas da sua eficácia. Talvez estejam ainda a aguardar o desenvolvimento do mercado. Embora, pelos padrões do setor segurador, o seguro de riscos cibernéticos seja uma linha de negócio nova, a maior parte das pessoas ignora que este tipo de seguro já é subscrito, sob várias formas, desde a década de 1990. Contudo, só nos últimos 10 anos, ou pouco mais, é que o mercado cresceu exponencialmente, com uma panóplia de seguradores e produtos a surgir no mercado para o cliente empresarial. O aumento dos ciber-ataques, a legislação crescente que promove a segurança de dados e o

elevado número de perdas sofridas são os fatores chave que levam ao crescimento do mercado mundial de ciber-seguro. Acrescente-se a tais fatores o recente enfoque, ao nível dos Conselhos de Administração, no risco cibernético, bem como as crescentes obrigações contratuais de aquisição da cobertura, pelo que se pode esperar que a procura de seguro para este tipo de risco continue a subir.

A Munich Re estima que o mercado global de seguro de ciber-risco tenha um volume atual superior a 7 mil milhões de dólares. A América do Norte continua a ser o mercado mais forte, representando 5,3 mil milhões dessa soma. O valor do mercado ciber europeu em 2020 estimava-se em mais de mil milhões de dólares. Muitos comentadores antecipam que o valor total do mercado chegará a 39,5 mil milhões até 2028. Se compararmos, por exemplo, o volume total atual de prémio de seguro D&O (cerca de 20 mil milhões de dólares) com os números acima, podemos ver que existe um imenso potencial de crescimento.

Espero poder dar ao leitor uma visão simples mas informativa sobre a cobertura disponível e a proteção que esta lhe traz. Com este conhecimento, espero que possa tomar uma decisão informada sobre o valor do produto e o seu lugar nos programas de gestão de risco cibernético.

II. O que cobre uma apólice de seguro de ciber-risco?

Como tem evoluído a cobertura?

Como em muitas outras linhas de negócio, as apólices de seguro de riscos cibernéticos têm mudado ao longo do tempo e a cobertura oferecida evoluiu para responder a dinâmicas de mercado, mudanças na legislação e necessidades dos compradores. Por exemplo, em meados da década de 1990, existia a preocupação em proteger os prestadores de serviços de ligação à Internet (ISPs) e responder aos riscos associados com o erro de código do ano dois mil que afetaria o relógio e calendário interno dos computadores (em inglês, *the Y2K bug*). Esta nova fase viu nascer as apólices originais de seguro tecnológico que acabaram por se transformar nas apólices de ciber-seguro que hoje conhecemos.

Em 2003, o foco da cobertura deslocou-se para a responsabilidade civil por Intrusão Informática e Fuga/ Extração Ilícita de Dados e Privacidade. Na altura, um dos impulsionadores foi o Estado da Califórnia, que promulgou leis sobre a privacidade, tornando obrigatório o aviso aos

titulares de dados afetados. Foi igualmente nesta altura que surgiram regulamentos específicos para determinados setores, por exemplo, em relação ao setor de cartões de pagamento e também ao dos cuidados de saúde. (É interessante notar que o RGPD na Europa teve impacto semelhante na taxa de adoção de programas ciber a partir de 2018.)

Com o passar das décadas, a atenção deslocou-se mais uma vez. Os compradores mostraram maior preocupação com coberturas de danos próprios (*first-party*), como a recuperação de dados, recuperação de ativos digitais e perdas de exploração. O ciber-crime, como, por exemplo, a fraude via telecomunicações (ao que o quadro jurídico norte-americano chama *wire fraud*), a engenharia social e a extorsão tornaram-se mais frequentes em meados da década de 2010 e os seguradores responderam a esta necessidade. À medida que atravessámos essa década e entrámos nos anos 20, para além do ciber-crime, muitos compradores começaram a ver como componentes fundamentais em qualquer cobertura a falha de sistemas informáticos e as perdas de exploração daí decorrentes. Mais uma vez, o mercado reagiu, ampliando a cobertura.

Todas as apólices contra o risco cibernético são iguais?

Acontece o mesmo que em todas as linhas de negócio: nos pormenores é que se encontra a diferença. Há que entender que as apólices não são criadas iguais. Pode ser uma forma extremamente simplificada de o dizer, mas as seguradoras só cobrem o que quiserem cobrir! Por isso, é importante ler as cláusulas dos contratos para comparar e contrastar a documentação de cada seguradora.

Em geral, uma apólice de ciber-risco deve oferecer proteção em três áreas principais, nomeadamente: segurança de dados, integridade dos dados e, finalmente, disponibilidade dos dados. Estes são os componentes chave de cobertura a procurar na apólice que se pretenda adquirir. Por exemplo, se a integridade dos dados (confidencialidade) for comprometida por interferência indesejável, ou os sistemas da empresa não estiverem disponíveis para sustentar a efetiva operação do negócio (disponibilidade), a apólice deverá funcionar.

Acontece o mesmo que em todas as linhas de negócio: nos pormenores é que se encontra a diferença

As apólices contra risco cibernético oferecem serviços suplementares?

Sim. Um dos traços distintivos do ciber-seguro é o acesso do titular da apólice a um conjunto de peritos antes e depois do sinistro. Nos sinistros de tipo cibernético o tempo é um fator de elevada importância, por isso, saber que se dispõe do apoio de uma equipa altamente especializada é muito importante. Estas equipas, que incluem peritos forenses em tecnologias e segurança da informação, juristas e especialistas em relações públicas, assegurarão que a perda seja mitigada de forma eficaz e eficiente. Este tipo de recurso é de particular valor para as PMEs, que não teriam tipicamente acesso a recursos desta natureza no seio da empresa. Sejamos honestos; tenho encontrado PMEs que usam estes recursos quase como se fossem os seus prestadores de serviços de TI subcontratados externamente. Afinal, se os sistemas forem abaixo, quem melhor para contactar se não uma equipa de especialistas em tecnologias da informação?

Algumas das empresas utilizadas pelas seguradoras para resposta a ataques, são: Cyberscout, ReSecure e KROLL.

Muitas seguradoras também oferecem aos seus segurados acesso a portais online onde podem encontrar informação importante para ajudá-los a gerir o seu ciber-risco. Tais recursos incluem documentos sobre protocolos e políticas de segurança, planos de resposta a incidentes, regulamentos, conselhos de gestão de risco, vídeos para formação de pessoal e outros. Muitas oferecem ainda uma linha de assistência 24/7 para onde se pode ligar antes ou depois do sinistro. Considerando que estes serviços estão incluídos no prémio de seguro, destaca-se ainda mais a vantagem de adquirir um seguro contra riscos cibernéticos.

Muitas oferecem ainda uma linha de assistência 24/7 para onde se pode ligar antes ou depois do sinistro

Mais recentemente, as seguradoras começaram a oferecer ferramentas de gestão de risco mais sofisticadas aos seus clientes para os ajudar, por exemplo, a monitorizar vulnerabilidades nos seus sistemas. Com a crescente sofisticação dos atacantes, a indústria seguradora tem sido obrigada a responder com maior inovação às ameaças que se multiplicam.

Quais são então as principais coberturas disponíveis?

Como referi anteriormente, seguradores diferentes oferecem níveis de cobertura distintos. Mas podemos dar uma visão geral das principais coberturas que o mercado disponibiliza hoje.

Neste momento, gostaria de desmistificar um dos equívocos sobre a cobertura das apólices de riscos cibernéticos. Não se limitam a garantir a responsabilidade civil de penetração ilícita em bases de dados ou a oferecer proteção a empresas que controlam dados pessoais identificáveis. A cobertura também protege o segurado contra perdas causadas por falhas de sistema, danos no sistema, perdas de exploração e crime cibernético. Para enterrar ainda outro mito, a apólice cobre, também, ficheiros e dados em formato físico. Por isso, em caso de esquecimento de papéis confidenciais num comboio ou de roubo do carro, a apólice será ativada.

Porém, cabe aqui um aviso. Como sucede com qualquer seguro com um limite de indemnização agregado, é importante analisar de perto a forma como este limite da apólice é afetado, e como a franquia da apólice se aplica transversalmente às diferentes rubricas de cobertura. Eis alguns exemplos daquilo que devemos esperar:

- Para assegurar uma rápida interação do segurado com o seu grupo de especialistas, algumas seguradoras não aplicam franquia aos custos associados aos serviços iniciais de resposta;
- Outras garantem custos de notificação a terceiros afetados fora do limite da apólice.
- A maior parte das seguradoras aplica o limite de indemnização apenas uma vez relativamente a todas as secções da apólice. Mas algumas oferecem limites individuais por secção. Uma melhoria considerável;
- Há que ter em atenção a existência de sublimites na apólice relativamente a certas coberturas, como por exemplo a do crime cibernético;
- Limites relativamente às reposições de capital no período de vigência da apólice.

A maior parte das seguradoras de ciber-seguro optaram por uma abordagem modular às coberturas oferecidas, dividindo as suas apólices em riscos de danos próprios (*first-party*) e riscos de terceiros. Vejamos quais as principais coberturas oferecidas:

Coberturas de Danos a Terceiros

- Responsabilidade Civil Segurança e Privacidade e Custos de Defesa
  - Penetrações de segurança de rede;
  - Transmissão de código malicioso;
  - Dano, alteração, corrupção, eliminação ou perda de ativos digitais de terceiros;
  - Violação de direito de privacidade de terceiros ou funcionários;
  - Ataques DDoS, *Phishing*[1] ou *Pharming*[2].

1 - É o mecanismo de elaborar mensagens que usam técnicas de engenharia social de modo a que o alvo seja ludibriado 'mordendo o isco'. Mais especificamente, os atacantes tentam enganar os recetores de emails ou mensagens de Phishing para que estes abram anexos maliciosos, cliquem em URLs inseguros, revelem as suas credenciais através de páginas de Phishing aparentemente legítimas, façam transferências de dinheiro, etc. (In https://cncs.gov.pt/pt/glossario/#linhasobservacao)

2 - Uso de meios técnicos para redirecionar os utilizadores para páginas web falsas disfarçadas de páginas legítimas de modo a que esses utilizadores partilharem os seus dados pessoais. (In https://cncs.gov.pt/pt/glossario/#linhasobservacao)

- Custos de Defesa relativos aos Regulamentos de Privacidade, Coimas e Penalizações[3]
  - Multas, avaliações, encargos, reembolsos na indústria de cartões de pagamento;
  - Compensação a terceiros por meio de coima ou penalização da parte do organismo de supervisão;
- Responsabilidade Civil Multimédia
  - Infração de direitos de propriedade intelectual, direitos de autor, slogan ou marca registada;
  - Denegrimento da reputação, difamação, calúnia;
  - Sofrimento emocional e mental.

Indicadas acima estão as coberturas habituais de proteção relativamente a terceiros, mas algumas seguradoras ampliam as suas coberturas para incluir, por exemplo, responsabilidade civil contratual e responsabilidade civil dos administradores e gestores.

3 - Onde forem seguráveis por lei

Coberturas de Danos Próprios *(First-party)*

- Custos de resposta a sinistros cibernéticos incluindo
  - Notificação;
  - Monitorização de crédito;
  - Relações Públicas / comunicação de crise;
  - Investigação forense de TI;
  - Jurídicos.
- Danos no sistema e perdas de exploração
  - Perda de rendimento;
  - Despesas extra e adicionais;
  - Recriação / reposição de dados;
  - Reparação ou substituição de *hardware*;
  - Danos consequentes à reputação;
  - Ciber-terrorismo.

De notar que os danos no sistema e perdas de exploração podem ser desencadeados não só por ocorrências cibernéticas dolosas como também por falhas sistémicas acidentais. Este é outro componente-chave a que se deve estar atento nas cláusulas específicas que a seguradora apresentar. Muitos dos acontecimentos cobertos pelo mercado ciber têm sido resultado meramente de erro humano.

É importante também que o texto da apólice não só especifique que "o sistema do segurado" está coberto mas que a cobertura também abranja os sistemas de terceiros, por exemplo, os fornecedores de tecnologia do segurado. Em certos casos, as seguradoras irão além dos fornecedores de tecnologia e oferecerão cobertura condicional de perdas de exploração aos fornecedores nomeados.

Outra questão a que se deve estar atento é a exclusão de dispositivos não encriptados. Muitas apólices não funcionarão se, por exemplo, o computador portátil ou dispositivo móvel do segurado não estiver encriptado e perder dados. Mas, mais uma vez, nem sempre é esse o caso e deve-se procurar incluir esta cobertura.

- Crime cibernético ou informático
  - Perda de dinheiro, crédito, valores mobiliários, produtos, bens ou serviços do segurado ou de terceiro;
  - Furto de dinheiro da conta bancária pessoal de um executivo sénior;
  - Despesas causadas por ataque de *Phishing*;
  - Transferência de fundos de boa-fé para terceiro em resultado de comunicação fraudulenta ou enganadora;
  - Engenharia Social;
  - Ataque de *Ransomware*[4] ou extorsão com alvo específico.
  - Uso de recursos do sistema através de meios como *cryptojacking*[5] ou recrutamento do dispositivo para *botnetting*;[6]
  - Despesas causadas por usurpação de identidade.

4 - O Ransomware representa um tipo de malware (vírus, trojans, etc.) que infectam os sistemas informáticos dos utilizadores e manipulam o sistema de forma a que a vítima não consiga utilizar, parcial ou totalmente, os dados armazenados que estão armazenados. A vítima geralmente recebe um aviso de chantagem por pop-up, pressionando a vítima a pagar um resgate para recuperar o acesso total ao sistema e aos arquivos. (In https://cncs.gov.pt/pt/glossario/#linhasobservacao)

5 - O criptojacking (também chamado criptomineração maliciosa) é uma ameaça online emergente que se esconde num computador ou dispositivo móvel e que utiliza os recursos da máquina para "minerar" dinheiro digital conhecido como criptomoeda. Trata-se de uma ameaça crescente que pode afetar os web browsers, bem como comprometer todo o tipo de dispositivos, desde desktops e computadores portáteis, até smartphones e mesmo servidores de rede. (In https://cncs.gov.pt/pt/glossario/#linhasobservacao)

6 - Rede de computadores infetados [drones] por software malicioso e controlados à distância, sem o conhecimento dos utilizadores, com a finalidade de enviar mensagens eletrónicas não solicitadas, roubar informações ou lançar ciberataques coordenados. (In https://cncs.gov.pt/pt/glossario/#linhasobservacao)

Estas são as principais coberturas oferecidas. Contudo, é importante estar atento aos detalhes de qualquer clausulado duma apólice. As secções de definições da apólice devem ser cuidadosamente analisadas, pois muitas seguradoras têm interpretações diferentes dos eventos seguros e das condições da apólice.

Também aconselharia ter em atenção a existência de restrições retroativas à cobertura. Como um ciber-ataque é frequentemente descoberto muito tempo depois de ter ocorrido pela primeira vez, deve-se procurar adquirir uma cobertura retroativa plena, com efeitos anteriores à data de emissão da apólice. Isto é mais comum em apólices para PMEs, mas vale sempre a pena ter este facto em consideração.

No Apêndice, consideraremos alguns exemplos de sinistros cibernéticos e a forma como a apólice reagiu a esses incidentes. Espera-se assim dar ao leitor alguns exemplos concretos da forma como as coberturas discutidas anteriormente operam na sequência de um sinistro no domínio cibernético.

Quem são as principais seguradoras de ciber-risco?

O número de seguradoras a subscrever ciber-risco tem subido significativamente desde a década de 1990. Contudo, tal como acontece com outras linhas de negócio, os *players* no mercado também mudam, em consonância com os ciclos do mercado. À medida que aumenta o desfasamento entre os rácios de sinistralidade e o preço dos seguros, tenho visto MGAs *(Managing General Agents)* com dificuldade em sobreviver. A pressão crescente sobre as seguradoras generalistas tanto dos seus gestores como dos resseguradores também levam a correções no mercado e, em certos casos, à saída das seguradoras da exploração desta linha de negócio.

O ciber-seguro ainda é visto por muitas seguradoras como uma área de grande potencial de crescimento

Como já se disse, o ciber-seguro ainda é visto por muitas seguradoras como uma área de grande potencial de crescimento, apesar dos riscos inerentes. Seria impossível listar todas as seguradoras, em todos os territórios, que subscrevem seguros de riscos cibernéticos (bastaria

considerar somente o mercado do Lloyd's, onde estarão ativas neste momento umas 77 seguradoras que cobrem o risco cibernético!). De igual modo, o apetite de risco difere bastante entre seguradoras. Algumas favorecem as pequenas e médias empresas, outras subscrevem apólices em excesso e ainda outras preferem trabalhar com entidades maiores e mais complexas.

Há várias empresas que atuam neste espaço há muitos anos (ou aumentaram o seu envolvimento através de aquisições) e continuam a oferecer capacidades ciber aos clientes. Estas incluem:

AIG	Hamilton
Allianz	HDI
Arch	Hiscox
AXA XL	Liberty
AXIS	Munich Re
Beazley	Markel
W. R. Berkley	Renaissance Re
BRIT	Swiss Re
Chubb	Travellers
Canopius	TMK
CFC	QBE
CNA	Zurich

*De notar que várias destas entidades operam no Lloyd's.

Como evoluirá o mercado ciber no futuro?

É muito difícil responder a essa pergunta com algum grau de certeza. Hoje existem várias tendências evidentes que, creio eu, se manterão no futuro.

Correção do mercado - o mercado de seguros foi atingido por um número sem precedentes de perdas ao longo do último ano. As perdas decorrentes dos ataques de *Ransomware* cresceram exponencialmente, alimentadas em parte pela transição das práticas de trabalho motivada pela Covid-19 e a redução nos orçamentos de manutenção das TI. A disponibilidade de *bitcoin* para pagar resgates também torna a extorsão por canais eletrónicos mais atraente para os delinquentes devido ao anonimato que proporciona.

O mercado de seguros foi atingido por um número sem precedentes de perdas ao longo do último ano

Os sinistros demonstraram o desfasamento entre os prémios cobrados e o nível de risco potencial.

Os aumentos superiores a 100% nas taxas cobradas têm-se tornado habituais e acredito que os aumentos continuarão a ser um fator de relevo nos próximos anos. Devemos esperar uma forte contração na disponibilidade de capacidades existentes e um enfoque na colocação de capital pelas seguradoras em áreas onde podem esperar melhor retorno, por exemplo, apólices em excesso em vez das primárias. As franquias mais elevadas (aumentos de 300% na retenção não são fora do normal nesta altura), cláusulas de exclusão e sublimites mais baixos para as coberturas de risco elevado (como as relacionadas com *Ransomware*) também serão de esperar.

Enfoque na gestão de risco - as seguradoras analisarão em maior detalhe os controlos e políticas de vigilância implementados pelo segurado. Uma apólice de seguro de risco cibernético não pode continuar a ser a principal abordagem à mitigação do

ciber-risco pelas empresas. As seguradoras desejarão ver provas de que as empresas implementaram as práticas de gestão de risco certas, para continuar a oferecer níveis elevados de cobertura. As empresas que não optam pela abordagem certa ou que não mostrem vontade de implementar as soluções recomendadas terão dificuldade em obter cobertura.

Crescimento da influência dos fornecedores de soluções de segurança cibernética - as relações entre as seguradoras e os prestadores de serviços de mitigação de ciber-risco ou serviços de resposta ao mesmo incrementar-se-ão. A integração de ferramentas de monitorização e prevenção na oferta da seguradora ao cliente tornar-se-á norma. Estes serviços adaptar-se-ão a um ambiente de risco em mutação e também aos progressos tecnológicos. Estas ferramentas serão mais amplamente adotadas pelos maiores compradores de seguro contra riscos cibernéticos.

Distribuição de ciber-seguro - é provável que as seguradoras continuem a procurar métodos novos ou adicionais para distribuir o seguro contra riscos cibernéticos. Com o passar dos anos aumentarão os portais na internet, as *insurtech* e a integração de apólices de ciber-risco em programas de afinidade. Os canais tradicionais para o mercado irão prevalecer, naturalmente, mas a necessidade de aumentar a penetração deste produto encorajará abordagens inovadoras ao mercado.

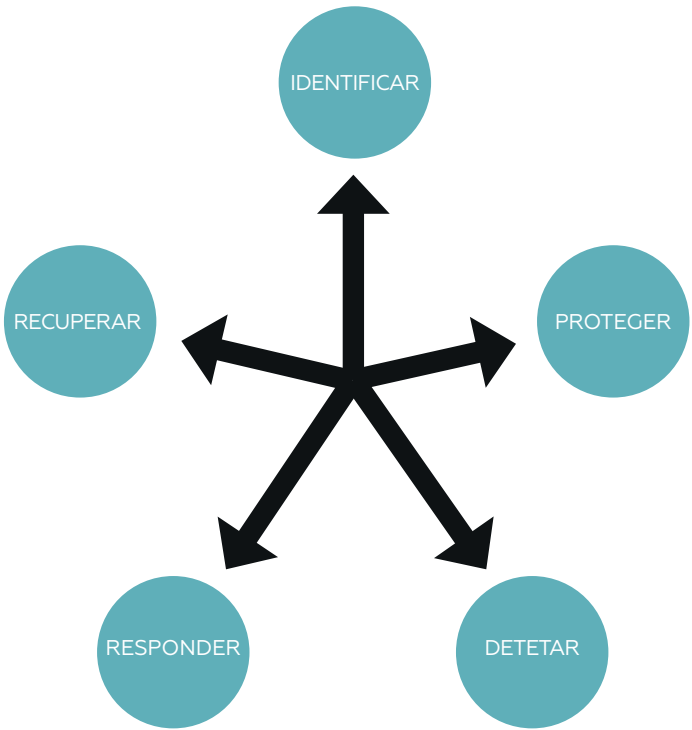
Intervenção e colaboração dos governos - com a mudança constante da paisagem geopolítica, a ameaça cibernética de origem estatal continuará a preocupar o mercado. O aumento da colaboração entre governos, organizações policiais e órgãos de segurança nacionais e o setor dos seguros precisará

de se intensificar. A informação sobre agentes maliciosos e os últimos tipos de ataque tecnológico deve ser partilhada mais abertamente com o mercado segurador e também com empresas de maior dimensão. Este processo deverá ser bilateral, devendo dispor-se o mercado segurador a partilhar o que aprende com novos sinistros que surjam. Os dados também terão de ser partilhados com fornecedores de modelação de dados para permitir a criação de modelos mais resistentes.

III. Considerações sobre a Gestão de Risco

Como devem as organizações abordar a gestão do risco cibernético?

Há muitos modelos e quadros de gestão de risco que podem ser seguidos aquando da elaboração de um programa de gestão de risco. Um desses quadros de ciber-segurança foi criado por um organismo do Departamento do Comércio dos EUA, o *National Institute of Standards and Technology* (NIST) [Instituto Nacional para os Padrões e Tecnologia]. Este quadro foi traduzido para várias línguas, entre elas o espanhol e o português, e reúne padrões, diretrizes e práticas que dão resultados efetivos em muitos setores, ajudando qualquer organização a compreender, gerir e reduzir o ciber-risco. O quadro abrange temas da tecnologia, da realidade física e dos trabalhadores, com um enfoque nos principais resultados da atividade económica. O núcleo do quadro inclui cinco funções de alto nível, como se verá abaixo:


IDENTIFICAR
RECUPERAR
PROTEGER
RESPONDER
DETETAR

Os gestores de risco que leiam este livro reconhecerão que várias das diretrizes relativas à gestão de risco que constam deste quadro são muito semelhantes às de outras classes de risco, como os riscos patrimoniais.

Contudo, seria pouco prático num livro desta natureza aprofundar mais pormenores necessários ao desenvolvimento de um programa de gestão de ciber-segurança com base nas orientações do NIST. Mas, se uma organização seguir um quadro desta natureza, terá dado passos significativos no sentido de melhorar a sua ciber-segurança. Devemos também ter presente que muitas PMEs não teriam os recursos ou sofisticação necessários à implementação de uma abordagem completa de gestão de risco desta natureza. Mas qualquer organização pode, de certa forma, mitigar o risco considerando estes tópicos, quer subcontratem a gestão de serviços informáticos ou não.

Mas, se uma organização seguir um quadro desta natureza, terá dado passos significativos no no sentido de melhorar a sua ciber-segurança

Há muitas medidas rápidas que as organizações que desejem reduzir o ciber-risco podem adotar, como, por exemplo: manter atualizados o *software* e *hardware*; utilizar tecnologia de gestão de palavras-passe; fazer cópias seguras dos dados fora da rede da empresa; e utilizar autenticação de dois fatores. No mundo de trabalho à distância em que vivemos agora, é de importância crítica sensibilizar os trabalhadores para a segurança no domínio cibernético.

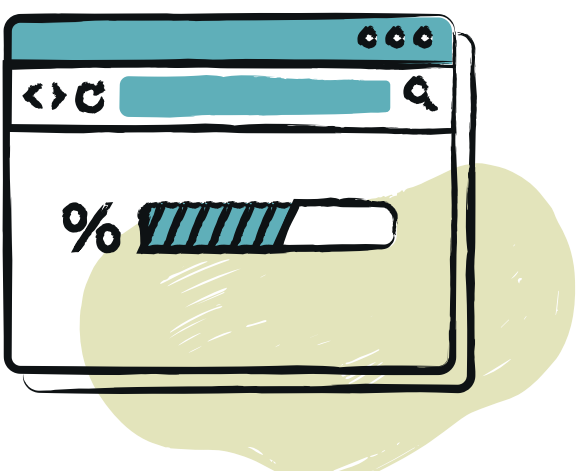
As práticas de gestão de risco influenciam os preços apresentados pelos subscritores?

Quando uma seguradora calcula o preço a cobrar pela cobertura de um risco, considera vários fatores que deviam ter sido contemplados por uma organização focada na gestão de risco. Observemos um exemplo utilizando alguns dos tópicos acima, que talvez possam esclarecer a forma como o enquadramento do risco e a subscrição de seguros poderiam ser conciliados.

Um subscritor que analisasse um novo risco consideraria o seguinte:

Cultura da organização e consciência do risco cibernético – a organização já identificou claramente, por exemplo, o tipo de dados que processa, armazena ou controla? E como estes dados atravessam a sua empresa e quem tem acesso aos mesmos dentro e fora da organização? Sabe quais são as suas "jóias da coroa" e o que pode motivar um ataque? Sabe quantos dos seus processos de importância crítica

são entregues a terceiros subcontratados? Culturalmente, educa os seus trabalhadores e principais *stakeholders* quanto aos perigos inerentes nos riscos como a engenharia social e a fraude via telecomunicações? O ciber-risco é levado a sério na empresa e considerado de uma forma positiva?



Nível de segurança em torno da sua infraestrutura de TI e dados – como é que a organização protege os seus dados tanto dentro da rede da empresa como quando transitam para fora dessa rede? Quem é responsável pela proteção e segurança dos dados, ou seja, usa-se uma organização externa para o efeito? A empresa usa encriptação? Usa autenticação de dois fatores[7]? Com que frequência procede a testes de penetração dos seus sistemas ou audita os seus protocolos de segurança? Atualiza regularmente o *software* para responder a vulnerabilidades ou pontos fracos conhecidos? Faz cópia de segurança dos dados? E onde armazena essa cópia de segurança?

Prontidão e resposta a incidentes – a organização tem um plano de continuidade operacional que inclua a resposta a um sinistro de origem cibernética? Delegou as responsabilidades dentro e fora da organização caso se dê um incidente? Testou o plano? Se sim, com que frequência? Como deteta a ocorrência de um incidente? Monitoriza regularmente os seus sistemas para tal efeito?

7 - Com o aumento recente de prejuízos causados por fatores cibernéticos, utilizar a autenticação de dois fatores começa a tornar-se um pré-requisito para muitas seguradoras.

Estas perguntas, como se pode ver, dariam a um subscritor uma compreensão aprofundada da abordagem da empresa ao ciber-risco. Se a empresa tiver adotado um modelo de gestão do risco como o proposto pelo NIST, os processos e procedimentos implementados levarão a respostas positivas às questões levantadas.

A apólice de seguro contra risco cibernético pode ajudar a aliviar algumas incertezas em torno do ciber-risco. A tranquilidade de saber, por exemplo, que existe uma equipa de especialistas à distância de uma chamada telefónica para ajudar a reagir a um sinistro na área cibernética, não tem preço.

Se uma apólice de ciber-risco fizer parte da estratégia de gestão de risco, complementará as funções de alto nível do programa, especialmente se ocorrer uma perda.

A tabela abaixo mostra como a apólice poderia complementar um programa de gestão de risco.

O Ciber-Seguro pode oferecer	Identificação / Consciencialização / Deteção	Proteção	Resposta / Recuperação
	Conselhos para a mitigação pré-sinistro	Tranquilidade financeira	Equipa altamente especializada em TI, Direito, RP e outras áreas, disponível para identificar causas e mitigar perdas
	Recursos de formação dos trabalhadores	Gestão de crises • Despesas de RP • Custos de Notificação • Monitorização de ID/ Crédito • Consultoria de Fraude	
	Ferramentas de planeamento de resposta cibernética	Perdas financeiras • Coimas e penalizações • Despesas extra • Perdas de exploração • Extorsão	Ajudar a organização a minimizar perdas de exploração e impactos regulatórios Conseguir os melhores resultados na sequência de crime cibernético
	Testes de penetração e instrumentos de monitorização de vulnerabilidades oferecidos por alguns seguradores	Responsabilidade Civil • Transmissão • Segurança • Privacidade • Propriedade Intelectual	Oferecer aconselhamento e apoio jurídico

IV. Conclusão

O ritmo da mudança no mundo tecnológico e a legislação sobre a privacidade dos dados levaram a um aumento da procura de seguros contra riscos cibernéticos. A cobertura e os preços disponibilizados pelas seguradoras nesta linha de negócio também mudaram ao longo do tempo para refletir as necessidades e a sinistralidade dos compradores.

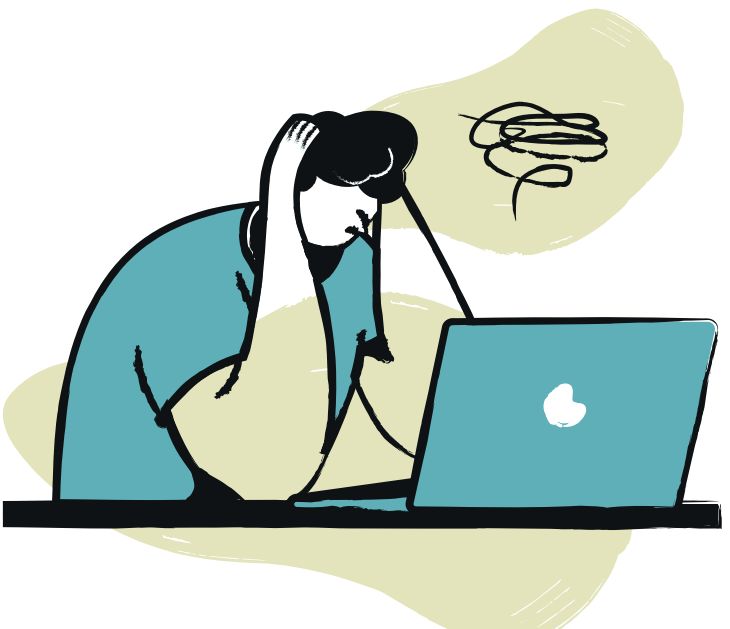
É importante que as empresas identifiquem e mitiguem as ameaças cibernéticas

É importante que as empresas identifiquem e mitiguem as ameaças cibernéticas que enfrentam diariamente, dada a dependência crescente do comércio na tecnologia. Não o fazer pode levar a consequências financeiras catastróficas.

O ciber-seguro pode desempenhar uma função de destaque na estratégica global de segurança cibernética, eliminando algumas das incertezas que se seguem a um sinistro no domínio cibernético. O apoio pré-sinistro também disponibilizado por muitas apólices pode ser de valor inestimável para as empresas que tentam gerir a sua exposição ao ciber-risco.

Espera-se que este livro tenha proporcionado uma perspetiva útil sobre este tema. Mais se espera que encoraje aqueles que ainda não adquiriram esta cobertura a encetar uma conversa com os seus consultores de seguros para saberem mais ou obter uma estimativa.

Como disse George Orwell, “Ver o que temos à frente do nariz é uma batalha constante”. No mundo do ciber-risco, esta batalha continua acesa.



Apêndice

Exemplos de Sinistros

É difícil, por vezes, determinar como é que as coberturas acima referidas reagem na realidade a um sinistro nesta área. Por isso mesmo, selecionámos alguns estudos de caso que, esperamos, possam demonstrar o âmbito da cobertura oferecida por uma apólice de riscos cibernéticos.

Setor do Sinistrado: Grupo Médico
Natureza do Incidente: Email de *Phishing*
Desembolso Total: $550,000

Garantias Ativadas: *Penetração e Fuga de Dados, Gestão de Crises, Engenharia Social, Coimas e Penalizações*

Um trabalhador de um grupo médico abriu inadvertidamente um email de *Phishing* que permitiu uma infiltração da rede do grupo. O programa antivírus não conseguiu conter o código malicioso. Dados pessoais identificáveis, incluindo nomes, moradas, informação e diagnósticos médicos de mais de mil pacientes foram expostos. Foram nomeados um perito em informática forense e uma empresa de relações públicas. Todos os indivíduos afetados foram notificados. O Gabinete de Direitos Civis lançou uma investigação e o grupo médico foi multado por permitir acesso não-seguro à sua rede.

Setor do Sinistrado: Serviços Financeiros
Natureza do Incidente: Transferência Inadequada de Fundos
Desembolso Total: $225,000

Garantias Ativada: *Penetração e Fuga de Dados, Gestão de Crises, Engenharia Social e Crime Informático*

Uma empresa de serviços financeiros foi vítima de um ataque via engenharia social que resultou numa transferência fraudulenta de $200,000. A transferência de fundos realizou-se mediante a receção de instruções de pagamento atualizadas que supostamente vinham de um fornecedor da empresa. A empresa transferiu os fundos para supostamente completar uma transação imobiliária.

Não se descobriu que a transferência bancária era fraudulenta até meses mais tarde, quando o destinatário notificou o segurado de que não tinha recebido os fundos. A empresa contratou advogados especializados em questões de privacidade e peritos forenses para investigar o incidente.

Adicionalmente, este sinistro ativou a garantia de Engenharia Social.

Setor do Sinistrado: Hotelaria e Restauração
Natureza do Incidente: Penetração e Fuga de Dados
Desembolso Total: $80 milhões

Garantias Ativadas: *Penetração e Fuga de Dados, Gestão de Crises, Coimas da Indústria de Cartões de Pagamento (PCI) e Custos de Privacidade*

Este sinistro envolveu a penetração de dados sobre cartões de crédito numa cadeia hoteleira. O hotel foi notificado pela Visa em duas ocasiões distintas sobre uma infiltração potencial de dados de cartões de crédito. O hotel contratou uma sociedade de advogados que, por sua vez, recorreu a especialistas forenses para conduzir uma investigação. Identificaram duas intrusões com impacto em mais de 300 000 cartões de crédito. Os custos totais incluíram a notificação de indivíduos afetados, custos de defesa, compensação financeira a indivíduos afetados e multas e penalizações PCI.

Setor do Sinistrado: Fabricante Farmacêutico
Natureza do Incidente: Ataque de *Ransomware*
Desembolso Total: $1 milhão

Garantias Ativadas: *Penetração e Fuga de Dados, Gestão de Crises, Extorsão por Via Informática e Ransomware. Perdas de Exploração e Despesas Extra*

Este incidente envolveu um fabricante especializado em equipamento para empresas farmacêuticas. A empresa sofreu um ataque de *Ransomware* que infetou a sua rede. As operações cessaram em resultado desse ataque e foi exigido um resgate equivalente a $500,000 em *bitcoin* em troca das chaves de decriptação. A empresa pagou o resgate. A seguradora contratou uma sociedade de advogados, fornecedores de serviços forenses e, especificamente, um fornecedor com capacidade de rapidamente providenciar grandes montantes em *bitcoin*. Os custos totais deste sinistro incluíram os custos legais e forenses além do pagamento do resgate.

Setor do Sinistrado: Município
Natureza do Incidente: Ataque de *Ransomware*
Desembolso Total: $225,000

Garantias Ativadas: *Penetração e Fuga de Dados e Gestão de Crises*

Tornou-se aparente que um número significativo dos servidores da escola do município tinham sido infetados por um programa malicioso quando numerosos utilizadores se queixaram de problemas em reiniciar computadores. Foi ativada a cobertura de danos próprios *(first party)* ao abrigo do acordo de seguro de Custos de Penetração e Fuga de Dados e Gestão de Crises. O segurado contratou advogados especialistas em privacidade e serviços forenses para investigar e remediar. Em seguida, foram notificados os indivíduos afetados, sendo-lhes providenciados serviços de atendimento por uma central telefónica e monitorização de créditos.

Setor do Sinistrado: Marca Distribuidora de Perfumes a Retalho
Natureza do Incidente: Engenharia Social e Furto de Fundos
Desembolso Total: $100,000

Garantias Ativadas: *Engenharia Social, Crime Cibernético e Penetração e Fuga de Dados*

Foi enviado um email falsificado ao gestor de contabilidade do segurado solicitando o pagamento urgente a um fornecedor. O remetente prosseguiu, enviando faturas pendentes — mas fictícias — ao gestor, pelo que este autorizou duas transferências fraudulentas. Mediante investigação forense de TI, descobriu-se que os sistemas do segurado não tinham sido comprometidos. Contudo, tinham sido efetuados pagamentos superiores a $80,000 antes de a empresa poder cancelá-los.

Setor do Sinistrado: Organização sem Fins Lucrativos
Natureza do Incidente: Transferência Inadequada de Fundos
Desembolso Total: $800,000

Garantias Ativadas: *Penetração e Fuga de Dados, Gestão de Crises, Engenharia Social e Crime Informático*

Um banco alimentar de uma cidade sofreu uma infiltração que resultou na fuga de informação pessoal sobre dezenas de milhares de doadores. Dada a sofisticação do programa malicioso no seu servidor, o acesso à informação sobre os doadores teve lugar durante um período de três anos. Os dados pessoais incluíam nomes, moradas, números de cartão de crédito e débito, códigos de segurança e respetivas datas de validade.

Peritos em informática forense assistiram na investigação. O banco alimentar foi obrigado a notificar todos os doadores afetados e fornecer proteção de identidade e monitorização de créditos durante um ano.

Setor do Sinistrado: Fabricante industrial
Natureza do Incidente: Ataque de Programa Malicioso na Sede de Fornecedor
Desembolso Total: $5,000,000

Garantias Ativadas: *Penetração e Fuga de Dados, Gestão de Crises, Interrupção Condicional da Atividade Operacional*

Um fornecedor externo do segurado sofreu um ataque de um programa malicioso que interrompeu as atividades de fabrico durante mais de duas semanas. Engenheiros e informáticos trabalharam incansavelmente para reparar os sistemas afetados e reiniciar a produção. Em resultado do ataque informático nas instalações do fornecedor, o segurado ficou sem acesso a componentes de importância crítica e as operações de fabrico foram interrompidas. A cobertura de Perda de Lucros / Risco de Contingência tinha sido adquirida pelo segurado e a seguradora pagou a perda de rendimento do fabricante e despesas extra decorrentes da falha na empresa do fornecedor externo.

Setor do Sinistrado: Sociedade de Advogados
Natureza do Incidente: Extorsão por Via Informática
Desembolso Total: $2.6 milhões

Garantias Ativadas: *Penetração e Fuga de Dados, Gestão de Crises, Extorsão por Via Informática e Ransomware. Perdas de Exploração e Despesas Extra*

Uma organização criminosa desconhecida obteve acesso à rede de uma sociedade de advogados. Pensa-se que conseguiram obter informação privilegiada sobre clientes, incluindo o nome de um alvo de aquisição de uma grande empresa cotada em bolsa, informação sobre uma patente de um cliente e ainda o prospeto de um cliente na área de capital de risco. Havia também uma grande quantidade de dados pessoais identificáveis pertencentes a grupos em ações judiciais coletivas. A firma recebeu subsequentemente um pedido de resgate no montante de dez milhões de dólares contra a ameaça de publicação de toda a informação na Internet.

A seguradora pagou dois milhões em despesas associadas à investigação forense, negociações relacionadas com a extorsão, um pagamento de resgate, notificações, monitorização de crédito e identidade, serviços de reposição, e honorários de advogados independentes. A empresa recebeu também um pagamento por perdas de exploração superior a $600,000 devido a perda de rendimentos e despesas extra associadas à intrusão no sistema.

Setor do Sinistrado: Contabilidade
Natureza do Incidente: Perda de Documentos
Desembolso Total: $700,000

Garantias Ativadas: *Penetração e Fuga de Dados e Gestão de Crises*

Um colaborador sénior, regressando a casa já tarde depois de uma reunião de trabalho, deixou a sua mala no comboio onde viajara. Sendo a época de revisão e ajuste de salários, a mala continha papéis que detalhavam a folha salarial dos trabalhadores, incluindo dados bancários, nomes dos trabalhadores, datas de nascimento, residências e números da segurança social.

Embora a mala nunca tenha sido encontrada nem tenha havido qualquer pedido de resgate, o segurado teve de notificar todos os colaboradores da fuga de informação, contratar advogados para monitorizar a situação jurídica e ainda oferecer serviços de monitorização de crédito. Alguns colaboradores afetados receberam compensação monetária. Embora se tenha pago $700,000 dólares até à data, o caso está em aberto na eventualidade de surgirem exigências no futuro.

Setor do Sinistrado: Construção
Natureza do Incidente: Envio errado de Email
Desembolso Total: Nenhum

Secções da Cobertura Ativadas: *Penetração e Fuga de Dados*

Neste caso, um email com pormenores da folha salarial de 60 trabalhadores foi enviado inadvertidamente pelo departamento de RH do segurado a todos os colaboradores noutra filial da empresa. O segurado notificou a seguradora. Contudo, após investigação, o segurado decidiu não tomar mais medidas. Não houve lugar a pagamentos. Incluímos este sinistro para demonstrar que por vezes as fugas de dados podem ocorrer por mero erro humano, mas nem sempre resultam num desembolso.

Biografia

Durante a sua carreira, de mais de 40 anos no setor segurador, Geoff Kinsella viveu e trabalhou num grande número de mercados de seguro e resseguro incluindo a Irlanda, Médio Oriente, Canadá e Reino Unido. Geoff viajou por todo o mundo e desenvolveu negócios em todos os continentes (menos na Antártida).

Tendo experiência em corretagem de seguro tanto como retalhista como grossista, compreende bem os desafios enfrentados pelos intervenientes no mercado de seguros.

Ao contrário do que diz o velho provérbio, segundo o qual "burro velho não toma andadura", Geoff decidiu concentrar a sua atenção em 2012 no mercado emergente do seguro de risco cibernético e em 2013 tornou-se sócio da Safeonline em Londres. Colocou ciber-seguro para diversas entidades, ajudou MGAs a encontrar capacidade de mercado e tem falado publicamente sobre este tema em muitos fóruns do mercado.

Geoff Kinsella desempenha atualmente funções de consultor junto de várias empresas.

Tem uma qualificação FCII, é acreditado pelo *Chartered Insurance Institute* do Reino Unido e titular de um Mestrado em Administração de Empresas (MBA).

MDS@2022

MDS GROUP

Brokerslink
Partner

Com a coleção Keep it Simple, de textos curtos e objetivos sobre temas relevantes do setor de seguros e risco, o Grupo MDS prossegue a sua missão de produção e partilha de conhecimento.

mdsgroup.com