MAIS

SEGURO

CYBER RISK

O ataque silencioso a empresas e pessoas

Novos riscos de mercado como o 'cyber' ainda não fazem parte das preocupações das PME, mas existem e são bem reais. Um ciberataque afeta a reputação de uma empresa, na medida em que tanto esta como os dados dos clientes ficam expostos. Perceber é o primeiro passo, e os seguros têm um papel a desempenhar na mitigação dos riscos.

ANÁLISE

Ciber-risco, como criar ‘awareness’ e sensibilidade para o risco

O desafio está lançado a seguradores e resseguradores. O ‘cyber risk’ continua no top 5 dos riscos atuais da humanidade, ao lado das alterações climáticas e das catástrofes naturais.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

O que diferencia um risco de outro é a tipologia que lhe está associada e é, sobretudo, o impacto na economia das empresas e das pessoas. Ora, o ciber-risco tem uma ligação estreita ao ciber-criminoso. E, tal como explica Manuel Coelho Dias, da Marsh Portugal, “falamos de pessoas ou entidades muitíssimo bem guarnecidas em termos de recursos informáticos e formação e, portanto, é fundamental que as entidades que investigam e combatem essa criminalidade o façam com iguais capacidades”.

Na mesma linha encontra-se André Paraíso Vicente, da AON Portugal, que realça o facto de o cibercrime ser a vertente do crime económico “que mais tem crescido em Portugal e no mundo”. Realça ainda que aquilo que está em risco não são apenas as instituições financeiras e as organizações que lidam com informações pessoais, porque o risco “estende-se também ao mundo físico, onde as interrupções elétricas, o encerramento de linhas de montagem, a violação de infraestruturas críticas e outras interrupções podem ocorrer como resultado desses ataques”. As perdas previstas até 2021, e decorrentes destes ataques, totalizam a nível global cerca de seis milhões de milhões de dólares americanos. As projeções são do mesmo grupo segurador.

Pedro Moura Ferreira da MDS, alerta para o facto do ciber-risco “minar de forma significativa a credibilidade das organizações, retrair a confiança dos clientes e testar a capacidade das empresas em resistir às constantes falhas de segurança, as chamadas *data breaches*, e aos crescentes ataques às suas operações de negócios”.

Mas se o medo se apodera das organizações, o que dizer dos indivíduos e das famílias? Sérgio Carvalho, da Fidelidade, diz que há o receio de que alguém se apodere de *passwords* para utilização abusiva, para além do perigo de circulação de emails que introduzem vírus e *malware* nos computadores ou com esquemas de burlas; a par do receio de assédio e danos morais, por invasão de perfis nas redes sociais e até acesso de estranhos a imagens pessoais através de *webcams* do computador ou de fotos publicadas online. Alerta ainda para o risco das compras online. Por seu lado, Sérgio Sá, da EY, salienta que a importância dos ciber-riscos é cada vez maior “devido ao papel da componente tecnológica”.

O cibercrime (é) a vertente do crime económico “que mais tem crescido em Portugal e no mundo”

Ainda assim, as projeções para o crescimento do negócio *cyber* são inferiores às estimadas e isso é explicado por João Madeira, da KPMG, que diz que “a perceção atual é de que as organizações ainda são predominantemente reativas, mas decorrente dos trabalhos que temos vindo a desenvolver e dos contactos que temos mantido, verificamos que a proatividade face ao risco de cibersegurança é uma realidade que veio para ficar, embora os investimentos em algo que nunca aconteceu sejam mais difíceis de justificar”.

Na mesma linha está Jorge Tobias, da Willis Towers Watson. Diz que “ainda não existe a perceção do valor que o seguro traz, mas, quiçá mais importante, ainda se desconhece o impacto financeiro que este tipo de fenómenos pode ter nas organizações. Para tomar decisões importa quantificar factos”. E ainda sobre o negócio para a indústria, Manuel Dias Coelho, da Marsh, conclui que o caminho futuro passa pela mutualização, assumindo que, no curto prazo, os ciber-riscos vão ser “uma linha deficitária” e isso deve-se à “tremenda incerteza que os eventos *cyber* representam, mas também aos *rates* baixos praticados na tentativa de captação de negócio”. Acrescenta que no médio/longo prazo, “a mutualização trará muitas vantagens ao tecido empresarial e, a seu tempo, rentabilidade ao mercado segurador”. ●

OPINIÃO

Será que possui efetivamente a melhor estratégia para combater o ‘cyber risk’?

PEDRO MOURA FERREIRA
MDS Technical & Placement Department | Director & MDS Claims Department | Director

O mercado atual, altamente global e interconectado, aumenta manifestamente a probabilidade de cyber risks. Hoje em dia, a dúvida sobre a existência de riscos de falhas de segurança e/ou ataques cibernéticos às organizações não é saber se existem, é saber quando vão acontecer.

Está provado que que o cibercrime não olha a sectores, dimensões, ou indústrias…

Um ataque de um hacker ocorre a cada 39 segundos. Simplesmente, não há como fugir.

A segurança cibernética é um grande problema e está em crescendo. As empresas estão com medo dessa ameaça potencial de segurança cibernética. O cyber risk é um assunto que mina de forma significativa a credibilidade das organizações, faz retrair a confiança dos clientes e testa a capacidade das empresas em conseguirem resistir às constantes falhas de segurança (data breach) e aos crescentes ataques às suas operações / negócios.

Vários estudos mostram que mais de 70% dos clientes dizem que deixariam uma organização após uma violação de dados. Se os clientes “cumprirem com a sua palavra”, qualquer empresa entrará em colapso em pouco tempo. Porém, verifica-se ainda hoje uma grande dissonância entre a preocupação manifestada com este tipo de risco e a prioridade que os próprios líderes das organizações dão na tomada de decisão sobre medidas estratégicas a adotar para a mitigação e transferência do risco.

Conhecer, estudar e avaliar o risco e a consequente exposição ao mesmo passa inevitavelmente por definir e implementar medidas de controlo e contenção do risco, intervindo sobre os fatores que o promovem e condicionam, como sejam, a vertente humana, física e digital, no qual incluímos naturalmente os softwares e hardwares, a segurança de processos e procedimentos, e claro, a formação das pessoas. A interrupção do negócio, as perdas financeiras, a perda de informação confidencial, o ataque à integridade de dados, a extorsão, o roubo de identidade, os danos reputacionais são alguns exemplos do impacto que um data breach poderá ter numa organização.

A gestão de risco / de crise é crítica para poder lidar com a materialização do risco, seja numa perspetiva de criar um plano de continuidade de negócio (plano de contingência), seja implementar instrumentos de financiamento e compensação de perdas através de seguros, o que constitui hoje um instrumento preferencial de “Risk Management” com significativa relevância na política de gestão empresarial.

O seguro Cyber dá cabal resposta a isto mesmo, garantindo a proteção do seu negócio, os custos relacionados com os danos e prejuízos sofridos na própria empresa, bem como as responsabilidades perante terceiros, daí que a procura por esta solução tem vindo a crescer.

O próprio mercado segurador oferece hoje soluções de seguro cyber para “todos os gostos e apetites” dos clientes. A grande amplitude de cobertura oferecida e o preço ainda reduzido do seguro face aos limites dados deveriam ser vetores valorizados pelos clientes.

Nos últimos anos verificamos que a própria evolução da solução cyber no mercado segurador deixou de ser vista e tratada como mais uma apólice de seguro para passar a ser um package onde é também oferecido um serviço. Atualmente, qualquer apólice de Seguro Cyber tem como diferencial a oferta de serviços adicionais focados na prevenção, monitorização, atendimento imediato pós-evento e um conjunto enorme de serviços especializados de informática forense. É de facto a materialização de uma tendência que se adivinhava… uma apólice de financiamento de risco e de serviço.

Nós, profissionais deste setor, temos sabido antecipar e responder aos diferentes riscos e necessidades dos clientes, funcionando, muitas das vezes na sombra, como o principal garante e motor das economias e sociedades. ●

FÓRUM COM CONSULTORAS

CIBERSEGURANÇA É PRIORITÁRIA NAS ORGANIZAÇÕES

As potenciais ameaças para as organizações nacionais e internacionais colocam a cibersegurança entre uma realidade que veio para ficar. E apesar de, por ora, as organizações ainda serem reativas, há uma cultura em mudança. VÍTOR NORINHA

NA ANÁLISE JUNTO DAS CONSULTORAS, O TEMA DA CIBERSEGURANÇA É CRUCIAL E ENCONTRA-SE NUM NÍVEL DE RISCO SEMELHANTE ÀS CATÁSTROFES NATURAIS E ALTERAÇÕES CLIMÁTICAS. A QUESTÃO REGULATÓRIA AINDA ESTÁ LONGE DE CONCLUÍDA NA UNIÃO EUROPEIA E ISSO CONSTITUI UM ÓBICE PARA UMA DISSUASÃO EFETIVA PARA QUEM ENTRA NESTE TIPO DE CRIME. A AJUDAR À PROTEÇÃO CONTRA O CIBER-RISCO ESTÁ O NOVO REGULAMENTO DE PROTEÇÃO DE DADOS. QUESTIONÁMOS AS CONSULTORAS SOBRE A TENDÊNCIA DAS EMPRESAS PARA DESCURAREM ESTE TIPO DE RISCO. LENTAMENTE, AS EMPRESAS ESTÃO A DEIXAR DE SER REATIVAS PARA SE TORNAREM PROATIVAS.

JOÃO MADEIRA
Partner
da KPMG

"Até 2019, o World Economic Forum tem vindo a classificar o risco de cibersegurança no Top 5 dos principais riscos globais, tendo uma classificação semelhante aos riscos de desastres naturais e alterações climáticas. Considerando o estado atual da maturidade de cibersegurança das organizações em Portugal assim como o aumento e evolução contínua de potenciais ameaças, acreditamos que o risco de cibersegurança deverá continuar a ocupar um lugar de destaque na lista de prioridades das organizações".

E sobre legislação para punir infratores "existe um forte movimento da União Europeia neste sentido (mas) a definição de legislação concreta para os diferentes tipos de ataques existentes é um processo evolutivo e de adoção gradual à semelhança do que tem acontecido com outras temáticas. Nos últimos anos, a concretização do Regulamento Geral de Proteção de Dados ("RGPD") e da Diretiva NIS, legislação relevante na União Europeia e com impacto ao nível da cibersegurança, demonstram o esforço e o caminho que está a ser percorrido no sentido de impedir ou, pelo menos, desencorajar ou dissuadir a ocorrência de ataques cibernéticos.

O RGPD é complementar a ações de proteção do risco de cibersegurança. O RGPD visa proteger de certa forma a informação crítica das Organizações, dos seus colaboradores e dos seus clientes, pelo que nada impede que os mesmos controlos sejam aplicados de forma mais abrangente nas Organizações, complementando os controlos de cibersegurança e ajudando à mitigação ou redução do risco de cibersegurança".

Mas as projeções para o crescimento do negócio *cyber* são inferiores às estimativas. "Infelizmente, a perceção atual é de que as Organizações ainda são predominantemente reativas, mas decorrente dos trabalhos que temos vindo a desenvolver e dos contactos que temos mantido, verificamos que a proatividade face ao risco de cibersegurança é uma realidade que veio para ficar, embora os investimentos em algo que nunca aconteceu sejam mais difíceis de justificar". Por outro lado "o sentido de "false safety" representa de certa forma ou é mais um dos indicadores do nível de maturidade do nosso mercado. A parte tecnológica em que normalmente os engenheiros informáticos atuam representa apenas uma das vertentes do risco de cibersegurança, sendo que uma efetiva gestão do risco de cibersegurança deverá ser feita considerando igualmente as vertentes de *governance*, pessoas e processos. A maioria dos ataques que acontecem hoje em dia são iniciados através do fator humano, pelo que o investimento ao nível da sensibilização e cultura de segurança deve ser igualmente uma área de foco e investimento.

É nosso entendimento que o papel do consultor passa por apoiar as organizações a dar os passos certos no sentido de se protegerem contra as ameaças de cibersegurança, sendo que isso implica apoio na definição e implementação de um processo de gestão de risco de cibersegurança que atua nas várias vertentes anteriormente mencionadas". E "decorrente de vários trabalhos que temos realizado nestas matérias para avaliação do risco de cibersegurança e apoio na contratação de seguros relacionados, verificamos que ainda não existe muita oferta no nosso mercado para este tipo de seguros, pelo que entendemos que é efetivamente uma oportunidade para as companhias que atuam nesta indústria."

MANUEL COELHO DIAS
Cyber Risk Specialist
da Marsh Portugal

"Os riscos movem-se num determinado plano e os danos noutro. Os ciber-riscos são difíceis de enquadrar na tipologia tradicional de danos. Repare que por via de um ciber-evento (que pode ou não ser um ataque) podem advir danos muitíssimos variados que vão da lesão de direitos de personalidade à paragem de negócio, sem esquecer despesas com a gestão da crise. E mesmo este quadro muito geral que lhe estou a dar, é altamente mutável em função da atividade concreta de cada empresa e do modelo de negócio desenvolvido pela mesma – naturalmente as ameaças e potenciais perdas de uma empresa de serviços B2C não são os mesmos de uma indústria pesada, ou ainda de uma instituição financeira. E não me parece que o problema seja falta de legislação. Há alguma desadequação da legislação, é certo, mas também repare que falamos de uma área permanentemente em evolução, e a lei tem que ser suficientemente flexível para enquadrar um sem fim de situações, e suficientemente clara para dar certeza e segurança aos cidadãos. Não se legisla de um dia para o outro. Do ponto de vista do poder público, penso ser muito mais preocupante a falta de meios das forças de segurança para responderem, quer em investigação quer em prevenção, ao cibercrime. Quando falamos em ciber--criminosos, falamos de pessoas ou entidades muitíssimo bem guarnecidas em termos de recursos informáticos e formação, e, portanto, é fundamental que as entidades que investigam e combatem esta criminalidade o façam com iguais capacidades. O paradigma do criminoso desleixado não representa, em regra, o hacker". Por seu lado, o RGPD "tem por objeto a salvaguarda da privacidade das pessoas singulares em ambientes digitais. O ciber-riscos, enquanto tópico da gestão corporativa, é incrivelmente mais abrangente do que isso. Engloba relações com fornecedores, gestão da cadeia de distribuição, controlo automatizado, entre muitas outras valências. É claro que ao exigir um determinado patamar de medidas técnicas e organizativas que garantam a segurança dos dados, e o exercício dos vários direitos ali previstos (portabilidade, apagamento, acesso), sem as quais não é possível assegurar um grau adequado de privacidade, o RGPD eleva a fasquia da segurança informática. A exigência de reflexão sobre o risco tecnológico que o RGPD impõe é, na minha perspetiva, muito positiva para a maturidade digital das companhias".

Relativamente ao tecido empresarial acho que há um caminho de sensibilização que está a ser

Dado Ruvic/Reuters

percorrido e tem demonstrado os seus resultados. Da nossa perspetiva, não interessa somente vender seguros, interessa que se crie uma awareness e sensibilidade para o risco. O grosso das PME começa agora, e após algumas perdas muito avultadas, a perceber que a gestão do ciber-risco é uma prioridade corporativa mesmo nos negócios mais pequenos: naturalmente o investimento não começa pelo seguro, começa pelas medidas de cibersegurança e organização interna. Estamos neste ponto com vários clientes que se encontram a fazer assessments em relação à sua exposição cyber e que num futuro próximo comprarão certamente o seguro. Também do ponto de vista do mercado, e embora estejamos ainda a viver um ambiente de prémios bastante competitivo, há algum cuidado na subscrição, o que exige por parte dos proponentes uma maturidade do risco que a maioria das empresas em Portugal não tem por defeito". Por outro lado, "penso que a visão sobre o risco cibernético está a mudar. Vemos cada vez mais as empresas a apostarem não só nas medidas técnicas de segurança, mas também na formação dos colaboradores como forma de prevenção, e no estabelecimento de cláusulas contratuais mais claras com os seus fornecedores e clientes. É um tema de risco integrado das organizações que não se compadece com mudanças do dia para a noite. *Baby steps.* O consultor é sempre um auxílio na perspetiva do conhecimento atualizado e sentido crítico que sempre deve aportar. Nesse sentido, o consultor atua muitas vezes como um *benchmark* para o cliente, vertido na visão que tem do setor e dos próprios pares da empresa a que se encontra a prestar o serviço. É também importante não esquecer que o consultor, pela natureza externa da sua atividade, acaba por estar numa posição mais confortável para sugerir e implementar mudanças. O modelo do one-shot change pode funcionar muito bem". E no futuro "estou convicto que o caminho dos ciberriscos passa pela progressiva mutualização. Não digo que não possa, no curto prazo, ser uma linha algo deficitária, seja pela tremenda incerteza que os eventos cyber representam, mas também pelos rates baixos praticados na tentativa de captação de negócio; no médio--longo prazo a mutualização trará muitas vantagens ao tecido empresarial e, a seu tempo, rentabilidade ao mercado segurador."

JORGE TOBIAS
Associate Director Corporate Risk and Broking da Willis Towers Watson

"Será difícil dizer que existe uma hierarquia ou escala comum de riscos para todas as organizações, contudo há um grau de exposição crescente e transversal aos chamados riscos cibernéticos. Haverá sectores específicos para os quais a gestão dos riscos cibernéticos assume elevada importância, podendo despoletar impactos a nível regulatório, operacional e reputacional. Outros porventura podem sofrer apenas impactos operacionais pelo que naturalmente falamos de diversas realidades, mas sem dúvida um risco transversal". Por outro lado, "a punição dos infratores será apenas uma das dimensões a observar. O papel preventivo e dissuasor da legislação assume, naturalmente, o seu relevo pese embora a aplicação territorial das leis seja um grande desafio. Quando temos hackers iranianos acusados pela justiça americana de desenvolver *malware* que serviu para colocar organizações americanas com o sistema informático inoperacional e aparentemente vemos o mesmo software malicioso utilizado em Portugal rapidamente percebemos a complexidade da questão.
A regulamentação (da proteção de dados) vai ao encontro da preocupação dos cidadãos e tem subjacente os princípios de "privacy by design and by default". Nesse sentido, claramente é convergente e vincula as organizações a princípios que talvez no passado não fossem considerados prioritários. Saber que dados tratam e para que efeito, obrigando em simultâneo que adotem boas práticas na proteção da informação é um passo na direção certa. Naturalmente o carácter dissuasor do regulamento (as famosas multas) é um incentivo à alteração de comportamentos e ao maior foco dado à salvaguarda dos riscos de privacidade e de segurança de dados". E sobre o futuro do negócio "ainda não existe a clara perceção do valor que o seguro traz, mas, quiçá mais importante, ainda existe desconhecimento sobre o impacto financeiro que este tipo de fenómenos pode trazer para as organizações. Para tomar decisões importa quantificar impactos.
Um exemplo disto que referimos: tivemos um cliente em Portugal que em 2019 (faturação anual entre seis e sete milhões de euros) foi vítima de um ataque de ransomware e apenas em custos diretos (reposição de sistemas e softwares, reconstrução de dados e gastos com consultores de IT) incorreu em gastos de 2,5% do valor da sua faturação anual (não incluímos aqui perda de receitas, potencial perda de clientes, custos reputacionais nem impacto regulatório por perda de informação confidencial). Não tendo um seguro especializado estes gastos foram naturalmente suportados a 100% pela organização. Caso tivesse um seguro, provavelmente o prémio anual suficiente para acomodar este nível de gastos poderia situar-se entre os 0,1% a 0,2% da faturação anual. Sectores onde os riscos tecnológicos são vistos como cruciais (saúde, telecomunicações, financeiro, utilities, etc.) olham para o tema de outra forma e são já claramente compradores dos chamados seguros cibernéticos. Aliando a ausência de quantificação à ausência de conhecimento sobre as soluções que o mercado segurador faculta, resulta que a maioria das organizações ainda internalizam (muitas vezes por desconhecimento) os impactos decorrentes destes novos fenómenos". De frisar que "haverá certamente empresas que têm competências e recursos humanos e financeiros que lhes permitem atuar de forma mais proactiva que outras neste domínio, mas, como temos visto em casos que têm vindo a público, mesmo as grandes empresas e com elevado nível de investimento nesta área são também vulneráveis (veja-se por exemplo o caso da banca).
Complementarmente à efetiva mitigação de riscos poderá ser aconselhável avaliar algum tipo de estratégia de transferência de riscos para o mercado segurador naturalmente adaptável à realidade de cada organização". Do lado dos consultores "o papel será relevante para todo o tipo de organizações sejam grandes ou de menor dimensão. Auxiliar as organizações na análise de vulnerabilidades e na quantificação do risco, de forma a auxiliar a implementação de medidas de mitigação do risco e posteriormente definir a melhor estratégia de transferência de risco para o mercado segurador são aspetos em que um consultor como a Willis Towers Watson pode ajudar.
O mercado segurador irá assumir o papel fundamental que assume na gestão de outros tipos de riscos não apenas mitigando o efeito financeiro que estes eventos podem trazer para pessoas e organizações mas, também, fruto das regras de subscrição que implementam, contribuindo para uma disseminação de níveis mínimos de gestão deste tipo de risco auxiliando assim na prevenção."

SÉRGIO SÁ
Associate Partner da EY

"Embora existam agora outros riscos emergentes que estão na agenda do dia das organizações tais como: ambientais, sociedade, geopolíticos e económicos, a importância dos cyber risks continua a crescer devido ao papel cada vez maior da componente tecnológica nas mesmas. Os cyber risks são colocados como uma obrigatoriedade às organizações através dos reguladores sob os temas de Risco, Segurança da Informação, Privacidade e Continuidade de Negócio. E a União Europeia tem vindo a criar diversa legislação nesta área ex: Cybercrime Law, GDPR, Network and Information Security - NIS, Cybercrime Act, Cybersecurity Act... No entanto diria que a principal dificuldade é o tempo da sua operacionalização já que essa legislação requer a transposição para leis locais assim como uma boa coordenação e monitorização a nível local e da UE". Por outro lado, o RGPD "é apenas uma das componentes do risco cyber e que detalha aspetos na componente Privacidade. Para além desses, há que ter em conta os da Segurança da Informação (inclui Privacidade), Continuidade de Negócio e os próprios Riscos como um todo da organização (em que o risco Cyber é apenas um deles).
A cibersegurança nas organizações continua a ser uma necessidade pela obrigatoriedade das organizações estarem em conformidade com um conjunto de requisitos impostos pelos reguladores. No entanto devido ao rápido crescimento de cyber existe uma escassez elevada de pessoas especializadas nesta área, a nível mundial, o que limita o acompanhamento das necessidades do mercado assim como a qualidade do serviço. E os riscos cyber são mais do que uma questão tecnológica em que os engenheiros informáticos são apenas uma das partes envolvidas. A correta abordagem a estes riscos implica o envolvimento de toda a organização. Os riscos cyber têm de ser vistos no impacto que causam nos objetivos de uma organização e nesse sentido envolve múltiplas áreas de uma organização, passando pela: Administração, responsáveis de Negócio, Serviços, Comunicação, Jurídico, Recursos Humanos, Auditoria, Conformidade, Risco, IT, Segurança, Privacidade, Continuidade de Negócio". Por seu lado, "dado o rápido crescimento e constante alteração dos riscos Cyber (resultado das tecnologias emergentes), necessidades de transformação digital das organizações, diversidade das áreas envolvidas e escassez de recursos especializados as empresas consultoras podem ter um papel determinante na orientação das organizações. Possuem conhecimento e experiência que permitem as organizações ficarem mais rapidamente alinhadas com os requisitos do mercado".
De frisar que a oferta de Cyber--Insurance já existe há algum tempo. No entanto, "agora com cada vez maior obrigatoriedade de controlar o risco Cyber e sabendo que nem todos são possíveis de ser mitigados as organizações vão ter cada vez mais necessidade de transferir o risco para seguros (quando possível). De forma a orientar as várias partes envolvidas saiu em 2019 a ISO 27102 - Guidelines for cyber-insurance que permite orientar nos riscos que não são possíveis de evitar na totalidade, mitigar ou aceitar pela organização."

FÓRUM SEGURADORES

INDÚSTRIA ASSUME RISCO PURO MAS QUER CLIENTES PREVENIDOS

Dentro dos novos riscos que empresas e pessoas estão a incorrer, o 'cyber' assume proporções alarmantes porque cresce exponencialmente, afeta negócios e reputação, e pode inclusive interferir com a vida. VÍTOR NORINHA

O 'CYBER RISK' É UMA PREOCUPAÇÃO OU UMA OPORTUNIDADE? QUISEMOS SABER JUNTO DA INDÚSTRIA O QUE LEVA AS EMPRESAS A RESISTIR A UMA EFETIVA COBERTURA DO 'CYBER RISK', OU SE O 'UNDERWRITING' E O 'PRICING' SERÃO OS MAIS ADEQUADOS.

SÉRGIO CARVALHO
Direção de Marketing e Clientes da Fidelidade

"O cyber risk é uma realidade da qual temos que tomar consciência, enquanto cidadãos, empresários ou *players* de mercado - nesta posição já com o dever de pensar e desenvolver soluções capazes de prevenir e mitigar o risco. A sociedade atual está a transformar-se a uma vertiginosa velocidade obrigando todos, enquanto cidadãos, empresas ou organizações, de cariz público ou privado, a compreender as novas dinâmicas para conseguir dar resposta a novas realidades, novas exigências e a antecipar desafios.
As alterações são demográficas com o aumento da longevidade e a redução da natalidade, sobretudo no Ocidente; são sociais com a alteração das tradicionais estruturas familiares e o aparecimento de novas dinâmicas relacionais; são climatéricas com o planeta a dar resposta à humanidade e a confrontar-nos com fenómenos atmosféricos cada vez mais atípicos; são regulamentares, com a entrada em vigor de legislação mais rígida que impõe regras para maior proteção dos cidadão mas incutindo, por sua vez, maior receio, sobretudo às diferentes organizações e players de mercado, em relação às sanções pelo seu não cumprimento; são tecnológicas com o homem a chegar cada vez mais longe na utilização de ferramentas digitais que permitem, no limite, substituí-lo em muitas tarefas. E todas estas alterações trazem consigo transformações comportamentais com impacto na vida privada mas que, obviamente, incidem e obrigam a uma reação económica e social, à qual ninguém pode ser indiferente.
Quando tudo muda, também os riscos se alteram. E aqui o papel das seguradoras é fundamental. Há hoje novos riscos, como o cyber, para os quais os cidadãos e as empresas têm que estar preparados, sendo essencial despertar a consciência coletiva para a sua existência. A prevenção torna-se assim primordial para alertar para um mundo que está a exigir o despertar para novas realidades e uma consciencialização apurada de forma a podermos dar resposta a um amanhã que pode sempre surpreender.
De natureza conjuntural ou de caráter mais estrutural, as mudanças requerem tempo. Tempo de perceção, de compreensão e aceitação, de adaptação e depois de reação ou antecipação de forma a projetar o futuro.
Talvez as empresas portuguesas não estejam ainda plenamente conscientes da necessidade de proteger os negócios em termos de risco global e de se precaverem para os novos riscos que surgem, como os cyber. Até porque os riscos cibernéticos são muitas vezes silenciosos. Não só pelo desconhecimento, mas principalmente pela inexistência de transparência total na sua denúncia. O receio de perda de reputação profissional impede muitas empresas e profissionais de diferentes setores de assumirem publicamente que foram alvo de ataques cibernéticos e que, devido aos mesmos, os dados dos seus clientes foram expostos ou postos em causa.
Mas é exatamente neste contexto que as seguradoras, enquanto entidades também responsáveis pela sustentabilidade económica e social devem exercer o seu papel - alertando, prevenindo, criando soluções adequadas às novas realidades e apoiando os clientes ao longo de toda esta evolução".
E "uma das mais-valias dos seguros cibernéticos é exatamente assegurar a questão legal de proteção de dados e proteger os clientes, nomeadamente as empresas, contra eventuais ataques que causem a exposição e violação de dados pessoais de terceiros. O Fidelidade Cyber Safety disponibiliza aos clientes serviços de prevenção de riscos de proteção de dados. Através do site da Fidelidade as empresas podem, gratuitamente, realizar um diagnóstico do grau de conformidade com a legislação em matéria de proteção de dados, sendo posteriormente elaborado um relatório com indicação da respetiva conformidade, recomendações para cumprimento do RGPD e indicação das possíveis sanções que podem ser impostas em caso de incumprimento.
Para além disso, duas das coberturas bases do Fidelidade Cyber Safety visam exatamente proteger o segurado de eventual Incumprimento do Dever de Custódia de Dados de Caráter Pessoal e de Violação do Direito à Honra e Intimidade Pessoal de Terceiro.
O Fidelidade Cyber Safety da Fideliade é uma solução dirigida a PME porque foi neste segmento de mercado que detetámos o maior gap de proteção. As grandes empresas têm normalmente soluções muito específicas de proteção, nomeadamente internacionais.
Destinado a PME e disponibilizado exclusivamente online, em fidelidade.pt, o Fidelidade Cyber Safety beneficia das funcionalidades do novo simulador web que disponibiliza gratuitamente uma análise e diagnóstico simplificado de eventuais vulnerabilidades do site da empresa; uma análise e diagnóstico simplificado à rede informática da empresa; um questionário para que a empresa possa avaliar o seu grau de cumprimento dos requisitos legais em função do RGPD (Regime Geral de proteção de Dados) e ainda a simulação de uma solução ampla de proteção para riscos cibernéticos até 500 mil euros.
O Fidelidade Cyber Safety pode ser contratado de forma simples, uma vez que as suas coberturas e serviços estão disponíveis num único plano fechado e a PME apenas tem que escolher o capital mais adequado às suas necessidades.
A PME pode optar pela inclusão da cobertura facultativa de Perda de Lucros pela interrupção da atividade do segurado".
Por outro lado, "proteger as pessoas singulares deste tipo de riscos torna-se cada vez mais prioritário e, por isso mesmo, a Fidelidade desenvolveu uma solução específica para este perfil, a qual será lançada brevemente. O Cyber Famílias virá assim assegurar proteção contra algumas das maiores ameaças que põem em causa a segurança de muitas famílias.
Sobretudo porque, embora haja ainda grande desconhecimento face a estes riscos, através dos estudos e das pesquisas que realizámos, concluímos que existem alguns receios comuns entre a população, nomeadamente: medo de que alguém se apodere de passwords para utilização abusiva; circulação de e-mails que introduzem vírus /malware no computador ou com esquemas de burla; receio de assédio e danos morais, por invasão de perfis nas redes sociais e até acesso de estranhos a imagens pessoais através das webcams do computador ou de fotos publicadas online. E mesmos as compras online que hoje em dia são realizadas pela maioria da população podem constituir um risco no qual ninguém pensa. O Cyber Famílias será um seguro de muito fácil contratação, destinado a qualquer agregado familiar, mas pensado sobretudo para proteção dos menores que utilizam a internet, com garantias que assentam em dois eixos fundamentais: Proteção Jurídica e Assistência".

PEDRO MOURA FERREIRA
Diretor da MDS

"O cyber risk é, sem dúvida e em primeiro lugar, uma grande preocupação. Este tem sido precisamente o vetor que tem norteado a nossa intervenção no mercado enquanto consultores e gestores de risco e seguros, principalmente, junto do tecido empresarial português.
Com o constante aumento do número de dispositivos eletrónicos existentes (Internet das Coisas) e dos seus utilizadores, assim como dos negócios realizados online e das informações guardadas em rede, a segurança no Ciberespaço tornou-se definitivamente uma preocupação muito séria das pessoas, das empresas, dos governos e das nações, interferindo diretamente com a confiança nos sistemas. O cyber risk é um assunto que mina de forma significativa a credibilidade das organizações, faz retrair a confiança dos clientes e testa a capacidade das empresas em conseguirem resistir às contantes falhas de segurança (data breach) e aos crescentes ataques às suas operações / negócios. Esta guerra virtual (e muitas vezes silenciosa) é capaz de causar danos financeiros e reputacionais gigantescos às empresas e, por esse motivo, o risco cibernético é hoje um assunto debatido em todos os Conselhos de Administração de empresas.
Verifica-se ainda hoje uma grande dissonância entre a preocupação manifestada com este tipo de risco e a prioridade que os próprios lideres das organizações dão na tomada de decisão sobre medidas estratégicas a adotar para a mitigação e transferência do risco. A evolução dos resultados ao longo dos anos aponta para uma crescente atenção por parte dos decisores, porém, e tendo presente que este risco dificilmente poderá alguma vez ser totalmente eliminado, as empresas têm investido mais na prevenção. O problema não é tanto a falta de sensibilização, mas saber a melhor

forma de minimizar a probabilidade e o impacto de um ataque informático. É compreensível que a grande preocupação das empresas seja, em primeiro lugar, tentar evitar o ataque / um *data breach* e, apenas num segundo momento, assegurar que em caso de ataque os danos são o mais contidos possível. Conhecer, estudar e avaliar o risco - e consequente exposição ao mesmo - passa inevitavelmente por definir e implementar medidas de controlo e contenção do risco, intervindo sobre os fatores que o promovem e condicionam, como sejam a vertente humana, física e digital, no qual incluímos naturalmente os softwares e hardwares, a segurança de processos e procedimentos, e claro, a formação das pessoas. A gestão de risco/de crise é critica para poder lidar com a materialização do risco, seja numa perspetiva de criar um plano de continuidade de negócio (plano de contingência), seja na implementação de instrumentos de financiamento e compensação de perdas através de seguros". Por outro lado do mercado segurador "tem-se verificado que a exigência dos seguradores na "compra do risco" está, de facto, mais fina e rigorosa. Os requisitos mínimos e obrigatórios para a contratação do seguro são agora maiores e mais complexos, obrigando a um crescendo na maturidade de risco das próprias empresas.
Também se verifica que os preços praticados na contratação dos seguros (prémios dos seguros) têm vindo a aumentar como resultado direto da exponencial exposição ao risco do mercado empresarial e, por consequência, do custo crescente dos sinistros participados".
Mais. "Parece inegável que o conhecimento e sensibilidade das pessoas e empresas sobre as suas responsabilidades nesta área aumentou consideravelmente. Mas estar em compliance com um normativo legal não significa em caso algum que um risco possa por si só ter sido atenuado e/ou eliminado. Existindo exposição, o risco estará sempre presente. Enquanto profissional desta área de consultoria e gestão de risco, direi que ter hoje maior consciência sobre os perigos e as responsabilidades que sobre nós incidem, traduz-se objetivamente numa maior sensibilidade e conhecimento daquele que será o impacto financeiro e reputacional que uma falha de segurança sempre acarreta. Daqui se compreende que os cuidados a ter passam inevitavelmente pela sensibilização e consciencialização para o risco: nos dias de hoje, todos somos um alvo. É fundamental assegurar que o nível de proteção instalada internamente ao nível de sistemas, processos e pessoas existe, é eficaz e eficiente, que a empresa está em total conformidade com leis e regulamentos, e que tem um plano de resposta e de gestão de crise. Por isso mesmo, investir em cibersegurança é acima de tudo proteger o seu negócio e a sua vida. Tendo em conta a abordagem que temos feito junto do tecido empresarial em Portugal, verifica-se que cada caso é um caso e, por isso mesmo, as soluções taylor-made (de fato-por-medida) gozam naturalmente de maior eficácia e eficiência na resposta aos incidentes. A exposição ao risco é inevitavelmente diferente de empresa para empresa. Enquanto consultores e gestores de risco e seguros com créditos firmados nesta temática há já bastantes anos, fruto de uma vasta experiência e conhecimento sobre esta tipologia de seguros aliada à facilidade de acesso que temos ao mercado local e internacional, o Grupo MDS consegue sempre disponibilizar soluções de qualidade a preços muito competitivos.
Já o Website Hacking explora as vulnerabilidades dos websites, onde se inclui o simples congestionamento do site impedindo mais acessos, a introdução de conteúdos ilegais no site, o roubo e/ou alteração da informação exposta; etc. Acima de tudo, a diferenciação das soluções não passa pela dimensão da empresa, mas sim pela especificidade e diversidade dos riscos cyber a que a mesma está exposta."

ANDRÉ PARAISO VICENTE
Business leader na AON Portugal

"Existem hoje mais dispositivos conectados à Internet do que pessoas na Terra. Se é verdade que estes transformaram positivamente a forma como vivemos e trabalhamos, também o é que fizeram aumentar as oportunidades para os criminosos lançarem novos ataques cibernéticos. Por isso, não é de estranhar que as empresas estejam preocupadas com este fenómeno. Aliás, segundo o último Global Risk Management Survey, produzido pela Aon, o cibercrime surge pela primeira vez na lista de principais riscos para as empresas em Portugal e, a nível global, foi registado um nível mais baixo de preparação para lidar com este tipo de risco. O cibercrime é a vertente do crime económico que mais tem crescido em Portugal e no mundo. E importa referir que não estão em risco apenas instituições financeiras e organizações que lidam com informações pessoais. O impacto das ameaças cibernéticas estende-se também ao mundo físico, onde as interrupções elétricas, o encerramento de linhas de montagem, a violação de infraestruturas críticas e outras interrupções podem ocorrer como resultado desses ataques. Segundo outros relatórios recentes desenvolvidos pela Aon, prevê-se que as perdas decorrentes de ataques cibernéticos atinjam globalmente os 6 triliões de dólares até 2021. O impacto que isto representa para a sustentabilidade das empresas pode ser catastrófico se estas não adotarem mecanismos e procedimentos de avaliação, quantificação, mitigação e resposta a incidentes".
Por outro lado "num mercado global eminentemente competitivo e de incessante e instantânea circulação de informação, os efeitos de um ataque cibernético em muito ultrapassam a mera perda financeira. É a credibilidade da marca e a confiança por parte de clientes e stakeholders que é posta em causa. A sua recuperação é de maior incerteza e dificuldade. Apesar da maioria das empresas estar ciente desta ameaça, admitir que a mesma existe é diferente de encará-la da forma mais apropriada. Aliás, o último Global Risk Management Survey revela uma clara incapacidade das empresas para gerir adequadamente este risco. O facto de ainda não terem sido alvos de uma ameaça em específico, ou pelo menos de a mesma ter sido percecionada, bem como considerarem que estão devidamente salvaguardados e/ou que o investimento necessário é demasiado elevado, leva a que muitas empresas ainda não olhem para a devida mitigação do risco cibernético de forma séria e estruturada. Desde logo, há que partir da premissa que um ataque vai acontecer. Tanto ou mesmo mais do que a própria prevenção, as empresas deverão atender à forma como irão responder perante uma falha de segurança". E sobre preços "há diversas soluções existentes no mercado, sendo que um seguro competente em matéria de riscos cibernéticos vai muito para além da mera proteção e compensação de danos próprios e/ou indemnização a terceiros lesados, ou mesmo dos custos de defesa e com comunicação de crise. É um produto integrado que oferece acesso a uma rede de peritos e de resposta permanente a incidentes que de outra forma não estaria ao alcance, pelos seus custos e especificidades, de um grande número de empresas. Adicionalmente, a contratação de um seguro de cyber ainda que seja, indubitavelmente, um instrumento de proteção e resposta a incidentes muitos importante, idealmente deverá ser o culminar de um processo de *assessement* que identifique as vulnerabilidades da empresa em específico nas suas diversas dimensões. Em termos do nível de prémios praticados, existe claramente uma relação direta com o referido anteriormente.
Por exemplo, no caso da Aon desenvolvemos uma ferramenta designada de CyQu (Cyber Quotient Evaluation), que analisa o nível de preparação da empresa perante o risco de cyber, identificando os pontos de maior conforto, bem como as principais vulnerabilidades. Este assessment é feito em estrita colaboração entre a Aon e os decisores das áreas mais sensíveis da empresa, por forma a ter um quadro efetivo do nível de resposta da empresa perante um incidente informático, bem como na estruturação e/ou atualização de um plano detalhado de gestão de riscos cibernéticos, tendo em vista a devida proteção do balanço e continuidade da empresa. De igual forma, avalia o nível de risco e maturidade da empresa em comparação com os seus pares do sector, num exercício de benchmarking. A Aon disponibiliza a ferramenta de diagnóstico CyQu, mencionada, que culminará na negociação e contratação de uma apólice que melhor responda à efetiva exposição ao risco e principais vulnerabilidades de cada empresa. Outrossim, trabalhamos com os principais seguradores especializados no tema, sendo que para a região da EMEA detemos um produto de seguro direcionado para PME, em condições técnica e comercialmente vantajosas.
Este produto permite o acesso imediato a uma equipa de gestores dedicados através de linha telefónica e esse contacto irá despoletar a intervenção de profissionais de várias áreas cujo principal objetivo será o crisis management (num sentido bastante amplo) junto do Cliente que sofreu o ataque (localização da origem, medidas de contenção e mitigação dos danos, comunicação com as entidades reguladoras…). E ainda que a maior parte das soluções de seguro existentes no mercado esteja dirigida a empresas e organizações, efetivamente existem produtos estruturados para pessoas singulares. Aqui a tónica estará mais na proteção contra a perda financeira que poderão sofrer em virtude de um problema de cibersegurança. Não obstante, também há soluções que garantem a potencial responsabilidade perante terceiros, bem como os demais serviços de aconselhamento técnico, jurídico e resposta a incidentes. O próprio aconselhamento psicológico poderá estar garantido na apólice. De uma forma genérica, há que ter presente que a maior causa de incidentes cibernéticos é o erro humano. No caso das empresas, a gestão das ameaças causadas pelos colaboradores é ainda mais desafiadora se tivermos em conta que temos hoje uma força de trabalho cada vez mais móvel, que geralmente liga os seus dispositivos pessoais a redes de terceiros. Por exemplo, os hackers podem segmentar dispositivos pessoais com níveis de segurança mais baixos, como smartwatches, para obter acesso e atacar telefones, dados de e-mail ou outras fontes de informações comerciais confidenciais. Um programa integrado de segurança cibernética só o é se considerar as pessoas como um elemento chave na prevenção, mitigação e gestão dos riscos. A fórmula é simples: quantas mais pessoas, mais pontos de acesso e, portanto, mais vulnerabilidade aos riscos."

JOHANN KOPP
Diretor de Produto Empresas da Allianz Portugal

"De acordo com os dados recolhidos pelo Allianz Risk Barometer de 2019 (ARB), os incidentes cibernéticos continuam a subir de posição no ranking dos riscos corporativos de maior relevo em todo o mundo. Em cinco anos passaram da 15ª para a atual 2ª posição. Portugal é, infelizmente, um dos países da União Europeia que menos investe na cibersegurança. Todavia, a consciencialização dos efeitos potencialmente devastadores dos riscos cibernéticos está em crescimento exponencial e progressivamente estamos a assistir a um maior dinamismo no investimento generalizado em serviços de cibersegurança por parte das empresas e da sociedade em geral". Por outro lado, "o mercado segurador português está a caminhar progressivamente na especialização deste tipo de riscos, mas há ainda um longo caminho a percorrer, sobretudo comparativamente com o grau de especialização do mercado de ciber--riscos dos Estados Unidos, que representa 85% do mercado mundial. Mas foi a pensar NAS pequenas e médias empresas que a Allianz Portugal lançou em 2019 o Allianz Cyber Risks, que é um produto inovador, abrangente e com uma ótima relação qualidade-preço. O Allianz Cyber Risks é comercializado em quatro opções de venda, cada uma a pensar nas necessidades de segurança das empresas e sempre focado em duas vertentes: a prevenção e o pós ataque cibernético. No âmbito dos serviços disponibilizados, o Cliente poderá ainda aceder a uma plataforma digital interativa e segura, especializada em cibersegurança e que permite a gestão online e integrada dos serviços contratados, como um canal de contacto direto que responde a dúvidas e necessidades dos Clientes em matéria de cibersegurança. Acrescentar que o processo da subscrição pode variar em função da dimensão e as características da empresa. O Allianz Cyber Risks, por ser comercializado em módulos fechados, é um produto de fácil subscrição e de emissão imediata - o mediador consegue oferecer uma cotação em menos de 30 segundos."

ESTUDO

Cenário macroeconómico incerto condiciona seguradores

A confiança da indústria seguradora a nível do retorno dos investimentos está em queda. O estudo é da Schroders, inserido no "Institucional Investor Study", e refere-se aos objetivos previstos para 2019. Das 156 seguradoras internacionais inquiridas apenas 51% espera atingir as expetativas de retorno do investimento, o que compara negativamente com 54% dos inquiridos que tinham uma expetativa positiva em 2018, e 61% em 2017.

A degradação da confiança está relacionada com o ambiente macroeconómico incerto na economia mundial, e ainda com factos políticos e eventos mundiais. Dentro deste último fenómeno têm sido relevantes as catástrofes naturais e as alterações climáticas. Dos inquiridos, cerca de 57% espera retornos do investimento da ordem dos 5% a 9%, quando há dois anos esse nível de retorno era esperado por dois terços dos inquiridos.

A Schroders frisa que a indústria seguradora é "a classe de investidores institucionais inquirida menos otimista". As companhias indicaram ainda que pretendem diversificar a alocação dos ativos de forma a gerarem retornos mais elevados. Recorde-se que a indústria tem sofrido com a manutenção de um nível de taxas de juro zero ou negativo por parte do Banco Central Europeu.

Nas carteiras de investimento vai ter mais relevância o tema da sustentabilidade e as alterações climáticas, que passam a ter uma dimensão superior à estratégia corporativa e à corrupção. Relevante ainda é a forma como os reguladores dão importância à gestão dos riscos de sustentabilidade por parte das companhias. ● *VN*

OPINIÃO

As seguradoras vendem seguros ou experiências?

TIAGO PALAS SANTOS
Manager da área de seguros da everis IT

Quando compramos algo ou subscrevemos um serviço, esperamos que este corresponda integralmente à expetativa gerada e que seja consistente ao longo do tempo. Isto aplica-se a um eletrodoméstico, a um carro, a um serviço de telefone e a um seguro… No entanto, ao contrário do que acontece com os bens de consumo ou com os serviços lineares, como a oferta de energia, água ou televisão, a indústria seguradora tem de conseguir conjugar um variado número de operadores para conseguir prestar um serviço de qualidade, sem falhas, que corresponda à expetativa do cliente.

Vejamos o exemplo de um carro avariado em plena autoestrada. A resolução do problema passa por chamar um reboque e solicitar um transporte ou veículo de substituição e encaminhar a viatura para uma oficina. Quem já passou por esta experiência, sabe que esta é muitas vezes uma situação imprevisível… O reboque demora mais do que o desejado, o táxi chega mais cedo, enfim, circunstâncias que adensam o stress causado por um carro avariado e que comprometem a experiência de serviço. Os clientes querem retomar a sua rotina habitual o mais rapidamente possível e estas falhas de coordenação acabam por criar desconfortos e irritações, que podem ser evitados. Imagine agora que existia uma solução em que a chegada do reboque coincidia com a chegada de um Uber… Deixa de ser necessário o veículo de substituição e toda a burocracia associada aos rent-a-cars.

Facilmente se percebe por esta situação hipotética que uma seguradora é, para além de uma gestora de risco, a coordenadora de um ecossistema de prestadores de serviços, que procura orquestrar para oferecer a melhor experiência aos clientes.

Apesar da indústria seguradora ser das que mais rapidamente abraçou as virtudes da tecnologia, boa parte da referida coordenação é ainda feita de forma analógica, com métodos pouco ágeis. Vivemos a era da transformação digital, boa parte das soluções do nosso dia-a-dia encontram-se no nosso bolso, à distância de um clique, por isso, rapidamente se compreende que as entropias de coordenação associadas à prestação de serviços por diferentes agentes podem facilmente ser ultrapassadas com soluções digitais, plataformas eletrónicas, app's, que, para além da redução de custos, melhoram os tempos de espera e evitam descoordenações.

É conhecida a dificuldade das seguradoras se diferenciarem, ainda mais pela pressão que existe sobre as margens e pelo crescente sentido critico dos clientes, que, legitimamente, esperam dos seus parceiros soluções que não comprometam as suas rotinas e a sua qualidade de vida. Um desafio que constitui também uma oportunidade para as seguradoras se reposicionarem, se aproximarem dos clientes e reduzirem a sensibilidade ao preço. Estamos na viragem da década e se há altura para projetar o futuro, pensar em mudança e investir na reinvenção é agora. ●

É conhecida a dificuldade das seguradoras se diferenciarem, ainda mais pela pressão que existe sobre as margens e pelo crescente sentido crítico dos clientes, que, legitimamente, esperam dos seus parceiros soluções que não comprometam a sua qualidade de vida