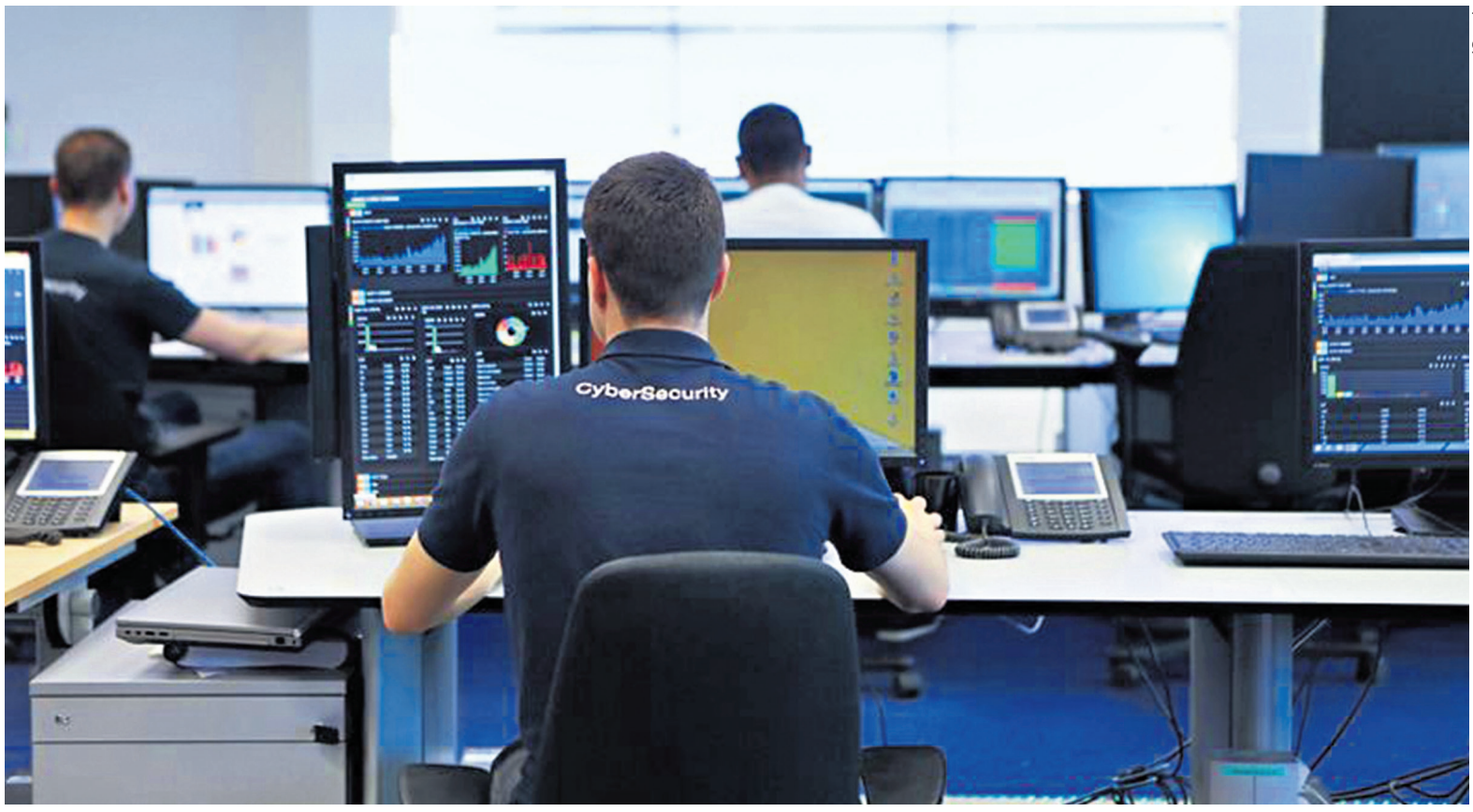
MAIS SEGURO

CYBER RISK

Mais digitalização significa maior risco

VÍTOR NORINHA
vnorinha@jornaleconomico.pt



iStock

A pandemia mudou as rotinas diárias para famílias e empresas e o novo paradigma "potenciou a exposição a riscos e vulnerabilidade no que à segurança cibernética diz respeito", sustenta Pedro Pinhal, da *broker* MDS Portugal. De acordo com o relatório de 2020 "Observatório de Segurança", do Centro Nacional de Cibersegurança Português, citado pela PwC, entre 2018 e 2019 houve um aumento do número de incidentes registados e do número de vulnerabilidades identificadas. E segundo o Eurostat, em Portugal, somente metade das empresas informam os seus empregados sobre as obrigações de segurança e apenas 41% destas realiza avaliações de risco periódicas para proteger a segurança face a incidentes. Adicionalmente, apenas 28% das empresas têm políticas e procedimentos de cibersegurança documentados. Revela ainda o website Builder Expert "Which EU Country Is Most Vulnerable To Cybercrime", Portugal é a 3.º maior vítima de cibercrimes na União Europeia. Diz Carlos Maia, da PwC, que "apesar de alguma sensibilização e alertas, no que respeita ao risco de ciberataques, muitas são ainda as empresas que permanecem inaptas para lidar com este tipo de riscos". As empresas, os colaboradores e a generalidade das organizações vão continuar a investir em processos, políticas e tecnologia. A pandemia intensificou a necessidade de digitalização nas relações comerciais e nas necessidades de fornecer melhores ferramentas aos colaboradores. O objetivo é melhorar, agilizar e tornar mais eficiente a cadeia produtiva. O reverso da medalha, afirmam os analistas, é o aumento do risco cibernético. Refere Pedro António, da Ageas, que "a descentralização do acesso à informação crítica de uma organização implica uma maior exposição aos riscos cibernéticos, pelo que será natural que se assista igualmente a um maior investimento e foco das organizações nesta área".

A função dos seguradores é desenhar um seguro tão completo quanto possível, "disponibilizando às empresas uma proteção ampla contra os principais problemas que lhes podem surgir pela frente e que decorram dos chamados incidentes cibernéticos", afirma Ricardo Azevedo, da Innovarisk Underwriting. Acompanhar as evoluções e tendências que vão sendo construídas à volta do risco cibernético é vital para adaptar as ofertas dos produtores de seguros a este tipo de incidentes. E isto porque deixou de ser relevante guardar o que está entre quatro paredes, mas antes o que está armazenado em discos, servidores ou na *cloud*. Um estudo feito em meados de dezembro pela multinacional de segurança Kaspersky indicava as ameaças financeiras para 2021, entre as quais se destacam o aumento das práticas de extorsão, na linha do que aconteceu recentemente com a EDP. Refere o mesmo estudo que os grupos especializados em *ransomware* aumentaram sistematicamente os montantes de resgate exigidos às vítimas, em troca da não publicação de informações que lhe foram sonegadas. Os especialista envolvidos no estudo "Kaspersky Vertical Threat Predictions for 2021" referem ainda que irá crescer o número de tentativas de extorsão como forma de obter dinheiro, e que as organizações serão o centro das atenções. E salientam que as empresas "podem sair ainda mais prejudicadas com a perda de dados e processos de recuperação exaustivos". Outro perigo para 2021 a nível cibernético será o furto de criptomoedas, com destaque para a mais popular, a bitcoin. Segundo os especialistas, a fragilidade económica de muitos países e a depreciação das moedas locais, levará ao aumento de situações de fraude/pedidos de resgate nos países que exijam bitcoins. ●

PUB

ANÁLISE

Pandemia criou condições para o aumento exponencial dos riscos cibernéticos

Até maio o gabinete de cibercrime da PGR tinha registado mais 139% de denúncias de crimes cibernéticos do que em todo o ano de 2019. A digitalização acelerada nas relações de trabalho estimulou os incidentes.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

A necessidade de informação e os receios quanto à pandemia estão a ser aproveitados por grupos maliciosos para ataques cibernéticos. Famílias, organizações e empresas são fustigadas por ataques oriundos de online *scams* e *phishing*, *malware*, *ransomware* e DDoS. Os seguradores estão a criar soluções e a alertar sobretudo as PME para o efeito devastador nos seus negócios. A área financeira, e em particular os bancos e as seguradores são as indústrias que registam o maior número de ataques, mas as notícias dão conta de ciberataques a organizações de saúde, autoridades policiais, forças armadas e organizações políticas.

Revela Pedro Pinhal, diretor da MDS Portugal, que "o número de incidentes cibernéticos em território nacional e no mundo têm aumentado progressiva e exponencialmente nos últimos anos. Se esta tendência era notória e preocupante, o surto pandémico que vivemos exacerbou-a para proporções nunca antes vistas e sequer antecipadas. Os cibercriminosos aproveitaram este novo contexto para lançar vários ataques, por exemplo, através de *malicious domains*, *online scams* e *phishing*, *malware*, *ransomware* e DDoS. A própria Interpol destacou que, no primeiro quadrimestre do corrente ano, foram detetadas 907 mil mensagens de *spam*, 737 incidentes referentes a *malware* e 48 mil endereços eletrónicos (URL) maliciosos – todos relativos à Covid-19.

A falta de um modelo de governação global para a tecnologia e de segurança cibernética aumenta o risco de um ciberespaço fragmentado e de regulamentações de tecnologia concorrentes

Aliás, já no presente mês de dezembro, a Unidade de Crimes Cibernéticos daquele organismo emitiu um comunicado internacional, através do qual alertou que foram identificados cerca de três mil sites associados a farmácias online sob suspeita de vender medicamentos ilícitos e dispositivos médicos e que 1.700 continham ameaças cibernéticas, como vírus informáticos. Relevantes também são os dados indicados por sites especializados que monitorizam o número de eventos cibernéticos maliciosos concretizados e tentados. Por exemplo, o site Kaspersky refere que ocorrem centenas de milhares de incidentes por dia em Portugal! Aliás, Portugal figura, diariamente, no top 30 no *ranking* de países que são alvo de maiores ataques/incidentes cibernéticos.

Este risco afeta de forma absolutamente transversal e global toda a sociedade e sectores da economia – sejam indivíduos, instituições públicas, pequenas ou grandes empresas". Adianta que o estudo "MDS Research - Situação Económica em Portugal" revelou que os empresários e gestores estão preocupados com a sustentabilidade dos seus negócios, identificando o risco cibernético como uma das principais ameaças.

Alvos em 2021

Os executivos nos sectores financeiro, telecomunicações e saúde acreditam que a desinformação e o *ransomware* irão aumentar no próximo ano. Nos sectores da energia, serviços públicos e recursos "existe um sentimento de poder vir a existir um impacto negativo significativo, maior do que aquele inerente a outras ameaças", afirma Carlos Maia, da PwC. Realça Manuel Coelho Dias, da Marsh Portugal, que "a pandemia aumentou a dependência dos canais digitais. E, portanto, um evento cibernético ganha maior destaque pela severidade que pode significar na operação das organizações. Empresas que até então tinham parte da sua cadeia de valor baseada em instrumentos não digitais, tornaram-se dependentes destes canais para poderem concretizar os seus negócios – é esta a situação de parte do comércio na medida em que o online se tornou a grande porta de venda de bens e serviços". Carlos Maia, da PwC, diz ainda que "devido à crescente digitalização e à maior interconectividade

global, os riscos cibernéticos estão a transformar os negócios e a economia global a um ritmo sem precedentes. A utilização generalizada de tecnologia tem vindo a aumentar o âmbito de oportunidades das empresas, para além dos limites geográficos e alterado significativamente a forma como estas gerem os seus negócios expondo-as a maiores vulnerabilidades e riscos".

A mesma fonte frisa que em 2020, o Fórum Económico Mundial, publicou o estudo "The Global Risks Report 2020" onde identificou os ciberataques como o risco tecnológico mais elevado e de maior impacto. "A falta de um modelo de governação global para a tecnologia e de segurança cibernética aumenta o risco de um ciberespaço fragmentado e de regulamentações de tecnologia concorrentes. Um ciberespaço fragmentado e padrões tecnológicos diferentes podem impedir o crescimento económico, exacerbar rivalidades geopolíticas e dividir sociedades", acrescente o gestor da PwC. Por seu lado, a EIOPA (autoridade europeia de supervisão dos seguros) tem vindo a analisar esta temática, tendo publicado em agosto de 2018 um estudo "Understanding Cyber Insurance - A Structured Dialogue with Insurance Groups" onde identificou a necessidade de uma compreensão mais profunda dos riscos cibernéticos e concluiu que estes representam o principal desafio para o setor de seguro cibernético europeu. Mais recentemente, publicou "Cyber Risk for Insurers - Challenges and Opportunities" onde explorou os desafios da cibersegurança, incluindo as práticas de subscrição das seguradoras neste tipo de riscos. Em Portugal, este tem vindo a ser um tema recorrente nos vários fóruns de discussão do setor segurador.

O valor da informação

"Atualmente, um dos ativos mais apetecíveis e de valor inestimável que uma companhia pode possuir, seja ela de seguros ou outra, é a informação. E é a informação que se traduza em vantagem competitiva, num mercado competitivo onde a alavancagem face à concorrência se obtém em qualquer fator diferenciador que cada entidade possa ter", diz a PwC. As companhias seguradoras constituem um alvo natural para ataques cibernéticos dado possuírem quantidades substanciais de informações confidenciais dos seus clientes. Por outro lado, a economia digital e o avanço da tecnologia oferecem oportunidades do lado da oferta de seguros *cyber*. De acordo com o Eurostat, apenas 10% das empresas com seguros contratados se protegem contra incidentes de segurança. Conclui a PwC que um mercado de seguros cibernéticos bem desenvolvido "para além de representar um potencial elevado de produção de novo negócio pode desempenhar um papel fundamental que permita a transição para uma verdadeira economia digital, aumentar a consciencialização sobre os riscos cibernéticos, partilhar conhecimento e melhores práticas de gestão de riscos cibernéticos e facilitar as respostas e a recuperação de efetivos ataques cibernéticos". Não sendo ainda um tema óbvio, ao analisar-se a oferta publicitada pelas seguradoras é, sem dúvida, um tema para o qual a sensibilidade e preocupação têm sido crescentes ao nível do setor segurador. A *broker* MDS saliente que foi o primeiro *player* do setor segurador em Portugal a ministrar formação e a criar uma solução para ajudar as empresas a protegerem-se em face do risco cibernético.

As informações mais recentes dão conta de que Bruxelas propôs o lançamento de uma rede de centros de operações de segurança em toda a UE baseada em inteligência artificial. O objetivo, diz a Lusa, é criar "um escudo de cibersegurnaça" para prevenir e responder rapidamente a ciberataques. E grandes empresas nacionais como a Sonae IM anunciou recentemente a consolidação dos seus investimentos em cibersegurança numa única holding estratégica, a Maxive Cybersecurity e que integrará a S21sec espanhola e a luxemburguesa Excellium. O objetivo é ter uma companhia que possa trabalhar todo o mercado europeu. E o relatório da multinacional especializada em inteligência e segurança de rede, a WatchGuard Technologies refere no "Internet Security Report" do 3º trimestre de 2020 que "os invasores continuam a visar redes empresariais apesar da adoção em massa do trabalho remoto, mostrando também um aumento dos demónios maliciosos e campanhas de *phishing* relacionados com a pandemia". Um dos especialistas da empresa refere, em nota, que os *hackers* estão a ajustar as suas táticas. Diz que as empresas devem "aumentar a proteção para o *endpoint* e para a rede" e esta deverá ser uma prioridade para 2021. Aconselha ainda o estabelecimento de uma "abordagem de cibersegurança por camadas, com serviços que podem mitigar ataques evasivos e encriptados, campanhas sofisticadas de *phishing* e muito mais". Pedro Matias, do grupo ISQ, refere que os sectores mais apetecíveis para ataques cibernéticos são a energia, saúde e transporte, banca e a própria indústria que entra na geração do IoT. E no mais recente relatório da multinacional de cibersegurança Kaspersky é referido que as ameaças financeiras em 2021 vão incluir extorsão, criptomoedas e ataques *web skilling*. E no modus operandi as previsões da empresa indica que haverá ataques MageCarting, ou seja, furtar dados de cartões de pagamento de plataformas de comércio eletrónico. Indica que os ataques serão executados do lado do servidor. Outro ataque acontecerá às moedas de transição. ●

Pandemia vai obrigar empresas a reavaliar o seu risco cibernético

CARLOS MARTINS
Diretor Geral

É seguramente reconhecido por todos que a utilização intensiva de novas tecnologias e de dispositivos inteligentes, a par do desenvolvimento de ecossistemas digitais e de novos padrões de comunicação como o 5G, por permitirem a recolha, análise e o tratamento automatizado de um maior volume de dados, fazem parte integrante e indissociável daquele que é o processo de transformação digital das organizações e da sociedade.

Esta aposta crescente na digitalização e conectividade, foi fortemente acelerada por efeito das medidas implementadas nos últimos meses para procurar mitigar os efeitos da presente pandemia, nomeadamente pelo recurso generalizado ao teletrabalho e pela transferência das operações de muitas organizações para o on-line, implicando novos e relevantes desafios para a gestão dos riscos cibernéticos, num momento em que se regista um aumento extraordinariamente significativo do número de ciberataques e sobretudo dos custos deles resultantes.

De facto, a dependência deste novo modelo de atuação descentralizado e digital, objeto de um cada vez maior escrutínio público e regulatório, tem inerente um vasto e complexo conjunto de novos riscos.

Apesar das organizações estarem cada vez mais cientes das potenciais ameaças cibernéticas aos seus ativos e negócios, a realidade é que existem naturalmente enormes diferenças entre as práticas de gestão dos riscos cibernéticos e daqueles que são considerados os riscos tradicionais, nomeadamente as resultantes da ausência de séries de dados históricos relevantes que permitam perspetivar, com elevado grau de fiabilidade, a severidade e a abrangência de futuros eventos cibernéticos.

No entanto, apesar de não serem facilmente mensuráveis, é certo que as consequências financeiras deste tipo de riscos, podem, num cada vez maior número de situações, revelar-se graves e até mesmo dramáticas para a continuidade das organizações, na medida em que têm de incluir, entre outras, a necessidade de dar resposta imediata a custos reputacionais, de notificação de clientes e da autoridade reguladora, de especialistas e peritos forenses para investigação, de respostas aos incidentes, de controlo dos danos e os decorrentes da responsabilidade por utilização e tratamento da informação, bem como a própria perda de lucros.

Neste contexto em que se regista uma rápida evolução nos cenários de exposição ao risco cibernético, importa que as organizações, independentemente da sua dimensão e do sector onde atuam, tenham conhecimento da possibilidade de robustecer substancialmente a sua proteção, transferindo para o mercado segurador, por um reduzido custo, de uma forma rápida e simplificada, um conjunto significativo destes riscos.

No caso concreto da SABSEG, em resultado do acompanhamento continuo e participação no desenvolvimento de produtos nesta área, disponibilizamos aquelas que são as melhores soluções de seguros para fazer face aos riscos cibernéticos, contribuindo assim ativamente para assegurar o reforço da proteção dos nossos Clientes.

SABSEG SEGUROS

Com o apoio

ENTREVISTA JOSÉ GALAMBA DE OLIVEIRA presidente da APS – Associação Portuguesa de Seguradores

O consumidor de seguros deve saber "identificar os principais riscos"

Os programas de literacia financeira não pretendem transformar o segurado num especialista, mas ensiná-lo a identificar os principais riscos.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

A literacia financeira é um dos temas relevantes nos seguros, mas o que significa não ter literacia financeira?
A falta ou a insuficiente literacia financeira traduz-se sobretudo na contratação de serviços financeiros sem que exista a noção do que se está a contratar. Os programas de literacia financeira da APS pretendem promover a aprendizagem sobre temas de seguro de modo a habilitar as pessoas a tomar decisões e efetuar escolhas informadas na área financeira. Não se pretende que cada consumidor seja transformado num especialista em seguros. Mas pretende-se que saiba identificar os principais riscos a que está exposto no seu dia a dia, que saiba que existem formas e meios para prevenir e mitigar esses riscos e, finalmente, que existem seguros que podem ajudar a enfrentar as consequências económicas que normalmente estão associadas à verificação do risco e que podem afetar os seus rendimentos e as suas poupanças. Por isso, os programas estão desenvolvidos para transmitir quer os conceitos mais básicos, quer informação mais desenvolvida e detalhada, consoante os níveis de conhecimento que cada público-alvo tem.
No final, o mais importante é proporcionar conhecimentos para uma adequada avaliação dos riscos e para que as pessoas sejam capazes de reconhecer as situações em que é relevante pedirem aconselhamento ou informação adicional. Essa necessidade de aconselhamento vai depender do seu nível de conhecimentos sobre o tema. Mas se tiverem os conhecimentos básicos sobre o que é mais relevante terem em conta quando contratam um contrato de seguro já se evitará que se contratem (ou que deixem de contratar) seguros sem terem noção do que podem ou não proteger através deste importante instrumento de proteção.

Para melhorar a literacia financeira da população não faria sentido começar por obrigar os seguradores a redigir contratos concisos e transparentes?
Os contratos são instrumentos jurídicos, que têm de respeitar os parâmetros e a linguagem prevista na própria lei e incluir todo o conteúdo que essa mesma lei obriga. No caso do contrato de seguro, estamos a falar de um contrato cujo conteúdo é extraordinariamente regulado pela lei e casos há, até, que está sujeito a cláusulas-tipo impostas pela lei ou pelo regulador. Claro está que esse contrato deve ser redigido da forma o mais clara possível, mas dificilmente será conciso devido à quantidade de informação que a lei obriga a que dele conste. E muitas destas matérias decorrem, até, de legislação comunitária e não apenas nacional. Mas, por isso mesmo, tão importantes como o contrato são os chamados documentos de informação pré-contratual que as empresas estão obrigadas a disponibilizar aos clientes, assim como a informação comercial que é veiculada pelas seguradoras, o próprio portal institucional e as novas *apps* que aquelas têm vindo a desenvolver e cujo objetivo é, precisamente, descodificar a linguagem mais técnica e jurídica e ajudar os consumidores a entenderem as condições dos contratos de seguro. Em Portugal, cerca de 75% das empresas de seguros desenvolvem já ações e programas específicos de transparência relativamente à terminologia e linguagem de seguros.

> "A falta ou a insuficiente literacia financeira traduz-se sobretudo na contratação de serviços financeiros sem que exista a noção do que se está a contratar

O conhecimento da literatura de seguros é hoje superior ao conhecimento existente há cinco ou 10 anos?
No que respeita a informação genérica sobre seguros, claramente. E a proliferação da informação na internet e nos canais digitais veio facilitar a disseminação desse conhecimento. O desafio aqui, como em qualquer outra atividade, é garantir que a informação veiculada nestes meios é a correta. Já no que respeita a estudos aprofundados sobre temas de seguros, seja na área jurídica, económica, social, na matemática ou até mesmo de história do seguro, há muito caminho para percorrer. É importante incentivar a escola e os alunos a investirem no estudo destas áreas ligadas ao seguro. ●

OPINIÃO

A cibersegurança começa em todos nós

MAFALDA CONTUMÉLIAS BATISTA
Managing Associate
Raposo Bernardo & Associados – Sociedade de Advogados

Nada mais oportuno do que abordar a problemática dos riscos cibernéticos num momento em que planetariamente toda a sociedade está a passar por uma transformação alucinante. A implementação do teletrabalho, decorrente da necessidade de garantir o distanciamento físico, obriga-nos a todos a fazer um uso muito mais intensivo da tecnologia.

Não obstante os riscos cibernéticos já fazerem parte do nosso léxico, em consequência de um acesso cada vez mais massivo à internet, com o consequente aumento do número de utilizadores, com a necessidade de guardarem e partilharem informações em rede, a segurança no Ciberespaço tem de passar a ser encarada pelas empresas, governos e cidadãos em geral, de maneira realmente séria.

O crescente número de ataques cibernéticos e a implementação do Regulamento Geral de Proteção de Dados justificam uma maior consciencialização por parte dos cidadãos e empresas para a adesão a um seguro que garanta uma resposta adequada aos riscos cibernéticos.

Nos dias que correm os negócios e a atividade das empresas passaram a assentar maioritariamente na tecnologia. A qualquer momento as empresas estão sujeitas a riscos sérios que podem causar danos de reputação empresarial, danos em relação a marcas, serviços ou produtos, violações de dados, com consequente insatisfação de clientes e perdas financeiras. Garantir a contratação de um produto de seguro apropriado pode minorar os efeitos associados a estas contingências.

Numa perspetiva geral, os ataques cibernéticos incluem, por exemplo, roubo de informações, divulgação de dados de clientes, fornecedores e colaboradores e até interrupção das atividades. Com esta amplitude e potencial gravidade, facilmente se percebe como é que o risco cibernético pode afetar de forma significativa a credibilidade das organizações, provocando a perda de confiança dos clientes e testando a capacidade das empresas em conseguirem resistir às constantes falhas de segurança.

O risco de um ataque cibernético é constante e permanente, até porque, na maioria das vezes, conta com a intervenção, mesmo que inconsciente, do fator humano. Mas isso não significa que não se possam tomar medidas para reduzir a exposição ao risco e evitar ou minorar os danos.

A abordagem mais adequada para lidar com estes riscos tem natureza preventiva: exige o envolvimento de toda a organização interna, através da sensibilização para a implementação das medidas de cibersegurança e avaliação do grau de cumprimento dos requisitos legais em função do Regulamento Geral de Proteção de Dados. Outra vertente de atuação passa pela implementação de ferramentas de compensação de perdas e danos sofridos na própria empresa, bem como das responsabilidades perante terceiros, através da contratação de seguros de riscos cibernéticos.

Paralelamente à realidade empresarial, os particulares encontram no mercado seguros que garantem proteção jurídica, assistência tecnológica e mesmo assistência psicológica. Uma boa atitude perante as exigências da cibersegurança começa em cada um de nós, ao lhe atribuirmos toda a importância que merece. ●

> O risco de um ataque cibernético é constante e permanente, até porque, na maioria das vezes, conta com a intervenção, mesmo que inconsciente, do fator humano

ENTREVISTA PEDRO MATIAS presidente do Grupo ISQ (Instituto de Soldadura e Qualidade)

"Ciberataques adequaram-se às condições do teletrabalho"

Ciberataques levam tempo a ser detetados e alguns passam despercebidos. A formação foi adaptada à nova realidade laboral, diz Pedro Matias.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

Qual o impacto da pandemia a nível dos riscos cibernéticos?
As empresas têm normalmente as suas redes protegidas mas não estavam preparadas para de um dia para o outro ver muitos dos seus colaboradores conectarem-se em redes públicas desprotegidas e incontroláveis que depois "ligam" à rede da própria empresa. A pandemia alimentou, desta forma, condições a alvos de ataques cibernéticos mais vulneráveis.

Há maior sofisticação nestes ataques?
Sim, os ataques adequaram-se às condições de teletrabalho. Ataques de *phishing* com novos métodos que aproveitam o trabalho hoje efetuado remotamente. Ataques de intrusão facilitados pela lacuna de segurança perimétrica e aproveitando depois as "portas de entrada" via VPN e via dispositivos móveis. Tal sofisticação faz com que, ainda hoje, alguns ciberataques levem tempo para serem detetados e outros passem até despercebidos. Daí a necessidade de existirem programas que ajudem e apoiem as empresas e a indústria a estarem protegidas destes riscos, como é o caso de um Projeto Europeu no qual o ISQ participa, o Encrypt 4.0 que visa exatamente a criação de uma *task-force* para a cibersegurança na indústria Europeia, para empresas no setor da manufatura, no âmbito da indústria 4.0.

Quais as entidades ou indústrias mais vulneráveis?
Temos de partir de um princípio básico: estamos todos vulneráveis. As entidades que já proporcionavam aos seus colaboradores uma importante mobilidade e que detinham departamentos de IT focados nessa realidade estão mais preparadas, mas também pode ser alvo. Os estudos revelam que os ataques cibernéticos se tornaram o novo padrão em sectores como energia, saúde e transporte, banca, sendo que a manufatura vem sendo cada vez mais afetada por estes ataques por causa da Internet das Coisas e da sensorização de sistemas com suporte em Web e mobile.

O que recomenda o ISQ para PME e instituições públicas?
Os gestores das PMEestão cientes dessas vulnerabilidades?
Sensibilização e mais sensibilização aos seus colaboradores sobre o tema. Normalmente a "fissura" do escudo contra os riscos cibernéticos é a parte humana de uma empresa. Claro, é também importante algum investimento em soluções que hoje existem no mercado que complementam as tradicionais "firewalls". No âmbito da nossa participação no projeto europeu Encryt 4.0, o ISQ desenvolveu uma Matriz de Risco de cibersegurança, que permite às empresas terem uma visão geral sistemática do cenário de risco de cibersegurança e a criação de perfis de risco precisos, em tempo real, de forma a possibilitar a adoção de medidas preventivas e a estabelecer medidas corretivas, em fábricas inteligentes. O ISQ vai também desenvolver laboratórios de capacitação online em cibersegurança, bem como uma ferramenta de acervo documental com casos reais de ciberataques que será alimentada e comentada em regime aberto.

Nos ataques cibernéticos realizados em Portugal são utilizadas as mesmas ferramentas que nos ataques feitos na Europa ou nos EUA?
No geral sim. Os ataques são normalmente "internacionais" pelo que existe um padrão de atuação com base em "normas" e "referenciais" internacionais.

Existem números de 2019 e 2020 sobre ataques em Portugal e as indústrias ou instituições envolvidas?
Existem estudos que comprovam que os ciberataques foram considerados as principais ameaças detetadas entre 2019 e 2020, segundo o ENISA, e que os mesmos estão entre os cinco principais riscos globais, segundo o Fórum Económico Mundial. ●

> "Temos de partir de um princípio básico: estamos todos vulneráveis

PUB

FÓRUM

INFORMAÇÃO É O MELHOR ATIVO DAS ORGANIZAÇÕES MAS TEM RISCOS

A utilização generalizada da tecnologia e de dispositivos inteligentes tem vindo a gerar mais riscos cibernéticos para as pessoas e para as organizações. Fomos saber quais as soluções disponibilizadas pelos seguros. VÍTOR NORINHA

QUISEMOS SABER JUNTO DE SEGURADORES E BROKERS QUAL O NÍVEL DE RISCO CIBERNÉTICO PARA PESSOAS E ORGANIZAÇÕES. QUESTIONÁMOS O SETOR SEGURADOR ACERCA DA ADAPTAÇÃO ÀS NOVAS CONDICIONANTES DO MERCADO; E FOMOS SABER COMO ESTÁ A EVOLUIR O RISCO E QUAIS OS PRINCIPAIS SERVIÇOS E INDÚSTRIAS QUE QUE SÃO ALVO DE ATAQUES CIBERNÉTICOS. E, POR ÚLTIMO, QUISEMOS AINDA SABER QUAL O IMPACTO DA PANDEMIA NO CRESCIMENTO DESSE RISCO E ATÉ QUE PONTO A DIGITALIZAÇÃO TEM DE ACELERAR.

CARLOS MARTINS
Diretor-Geral da Sabseg

"A identificação e a avaliação dos riscos cibernéticos faz parte integrante da cultura da nossa organização e atribuímos-lhe uma enorme importância na definição da política global de gestão de riscos. Neste sentido, temos vindo a reforçar o investimento nesta área, de modo a dispormos da estrutura de competências e recursos mais adequados para assegurar uma elevada segurança cibernética, além de, naturalmente, já há muito tempo termos optado pela transferência de uma parte destes riscos para o mercado segurador, através da subscrição de uma robusta apólice de seguro. E é indubitável que as ameaças decorrentes de incidentes cibernéticos estão a aumentar de forma exponencial em todo o mundo. Estamos perante um problema transversal a toda a sociedade, cujos alvos preferenciais têm evoluído dos indivíduos para as organizações, afetando os mais diversos sectores de atividade. A crescente utilização generalizada da tecnologia e de dispositivos inteligentes nos mais diversos domínios de atuação acarreta seguramente mais riscos numa fase em que as organizações e a sociedade avançam no seu processo de transformação digital. Por outro lado, a necessidade de assegurar a continuidade das operações de muitas empresas e instituições, de modo a limitar os efeitos da pandemia por Covid-19, implicou uma enorme dependência de novas formas de conectividade e de digitalização de muitos processos. Neste sentido, algumas das medidas implementadas nos últimos meses, de que são exemplo a opção pela adoção generalizada do regime do teletrabalho e pela migração para o on-line de muitas operações, potenciou um incremento considerável dos ciberataques e dos custos deles resultantes, bem como dos desafios que se impõem à sua gestão e mitigação."

CARLOS MAIA
Insurance Lead Partner da PwC

"Devido à crescente digitalização e à maior interconectividade global, os riscos cibernéticos estão a transformar os negócios e a economia global a um ritmo sem precedentes. A utilização generalizada de tecnologia tem vindo a aumentar o âmbito de oportunidades das empresas, para além dos limites geográficos e alterado significativamente a forma como estas gerem os seus negócios expondo-as a maiores vulnerabilidades e riscos. Um mercado de seguros cibernéticos bem desenvolvido, para além de representar um potencial elevado de produção de novo negócio pode desempenhar um papel fundamental que permita a transição para uma verdadeira economia digital, aumentar a consciencialização sobre os riscos cibernéticos, partilhar conhecimento e melhores práticas de gestão de riscos cibernéticos e facilitar as respostas e a recuperação de efetivos ataques cibernéticos. Não sendo ainda um tema óbvio, ao analisar-se a oferta publicitada pelas seguradoras é, sem dúvida, um tema para o qual a sensibilidade e preocupação têm sido crescentes ao nível do sector segurador. E à luz de alguns dos mais recentes eventos cibernéticos, as empresas, de todos os sectores, estão cada vez mais conscientes das potenciais ameaças aos seus negócios, bem como da necessidade de terem estratégias digitais, técnicas de mitigação de risco e modelos de segurança cibernética. Ataques, que geram manchetes e destroem marcas, têm vindo a demonstrar que estas ameaças estão a tornar-se mais sofisticadas e agressivas. De acordo com o mais recente estudo da PwC, Global Digital Trust Insights Survey 2021, nos primeiros três meses da pandemia, os CEO procederam a desenvolvimentos digitais nas suas organizações a uma velocidade surpreendente, avançando para o segundo ou terceiro anos de seus planos a cinco anos. O momento não poderia ser melhor para abordar tal tema. Estas mudanças recentes nos modelos / processos de negócios levaram muitas empresas a acelerarem os seus programas de digitalização. Nos tempos de incerteza em que vivemos, a probabilidade de um ataque cibernético é maior do que alguma vez foi. Este ano trouxe um aumento significativo do número de invasões cibernéticas, *ransomware* ou *malware* e violações dos dados, juntamente com um aumento nas tentativas de *phishing*.

MANUEL COELHO DIAS
Cyber Risk Specialist da Marsh Portugal

"O sector segurador lida com o risco cibernético numa dupla vertente: é ele próprio um alvo da digitalização e dos seus riscos e, por outro lado, está obrigado a oferecer aos seus clientes soluções de mutualização para fenómenos muito complexos e ainda algo incertos. Julgo que, nos últimos anos, temos assistido a um aumento interessante da oferta de produtos de transferência de riscos digitais, mas a incerteza ainda é muito grande e a maioria dos seguradores é bastante relutante na aceitação destes riscos. As perdas fruto de eventos cibernéticos têm crescido exponencialmente. *Ransomwares* e *data breaches* são neste momento ameaças sérias ao negócio das nossas empresas. O risco é maior também porque a dependência dos meios digitais cresce rapidamente, num ambiente tecnológico e económico altamente interligado. De acordo com o Relatório da Marsh sobre sinistros *cyber* na Europa Continental, publicado em agosto, os serviços financeiros lideram o *ranking* de sectores mais afetados, seguidos pela indústria (*manufacturing*). Por outro lado, a pandemia aumentou a dependência dos canais digitais. E, portanto, um evento cibernético ganha maior destaque pela severidade que pode significar na operação das organizações. Empresas que até então tinham parte da sua cadeia de valor baseada em instrumentos não digitais, tornaram-se dependentes destes canais para poderem concretizar os seus negócios – é esta a situação de parte do comércio na medida em que o online se tornou a grande porta de venda de bens e serviços."

RICARDO AZEVEDO
Diretor Técnico da Innovarisk Underwriting

"Hoje em dia todos os relatórios e estudos que são feitos sobre a temática do risco apontam a questão cibernética como uma das principais ameaças que pendem sobre a vida dos cidadãos, das empresas e das instituições e por isso, ao longo dos últimos anos, na Innovarisk temos olhado para este tema com especial atenção. Procurámos desde o primeiro momento desenhar um seguro tão completo quanto possível, disponibilizando às empresas uma proteção ampla contra os principais problemas que lhes podem surgir pela frente e que decorram dos chamados incidentes cibernéticos. Ao longo do tempo e atendendo a que estamos perante uma realidade que evolui de forma extremamente rápida, temos procurado acompanhar de perto as evoluções e tendências que se vão sentindo a nível de novas tecnologias, sistemas de segurança ou da tipologia e caracterização dos ataques cibernéticos. Essa informação permite-nos não só ir adaptando o nosso seguro à realidade e às necessidades de cada momento, como possibilita também que possamos aconselhar devidamente os nossos clientes tendo por base os principais riscos existentes e as melhores práticas em matéria de segurança de dados e de sistemas. Por outro lado, o mundo é hoje menos material e mais digital. Quando antes as empresas se preocupavam sobretudo com o que de valor guardavam entre quatro paredes, em estantes ou dentro de cofres, hoje têm que olhar também para o que está armazenado em discos, servidores ou na *cloud*. Para além disso, muitos equipamentos estão ligados à rede e é possível controlar a impressora do nosso escritório ou uma máquina de produção de uma unidade industrial, a partir de instruções dadas por um computador do outro lado do mundo. O risco é forçosamente maior e tão mais elevado quanto estivermos a falar de empresas e sectores mais dependentes de sistemas digitais para poderem operar, menos apetrechadas do ponto de vista da segurança informática ou que lidem com dados particularmente sensíveis. As empresas que se enquadrarem nesses casos ficarão sempre numa posição mais frágil perante um problema que surja, o que vai aliás fazer com que se tornem alvos mais apetecíveis de pessoas mal intencionadas."

PEDRO ANTÓNIO
Chief Future Officer do Grupo Ageas Portugal

"O risco cibernético sempre foi uma preocupação e a pandemia, com a necessidade de manter ligados à distância todos os intervenientes da

cadeia de valor (clientes, colaboradores, parceiros, fornecedores), veio reforçar o foco da organização nesta área tão sensível. Este reforço é materializado pelo investimento realizado em processos, políticas e tecnologia, contando, para além das nossas equipas internas, com a participação de parceiros especializados. E, naturalmente que o risco cresceu durante a pandemia e é expectável que se mantenha mais elevado com a tendência de aumento nas relações comerciais à distância. Todos os serviços e indústrias que, por um lado, começaram a ter um maior número de relações comerciais não presenciais e que, por outro lado, mantêm a cadeia de valor a funcionar de forma remota (colaboradores, parceiros e fornecedores), estão hoje mais expostos ao risco cibernético. É uma tendência que veio para ficar e caberá às organizações encontrarem os melhores meios e ferramentas para minimizar o risco de exposição. Por outro lado, a pandemia alterou-nos, de forma abrupta, hábitos de trabalho, consumo e mesmo de convivência profissional, não sendo previsível que no final da crise as relações comerciais e de trabalho voltem exatamente ao que eram no passado. É, por isso, expectável que as organizações intensifiquem os seus investimentos na digitalização das relações comerciais com os seus clientes, bem como na disponibilização de melhores ferramentas aos seus colaboradores para assegurar um modelo de trabalho remoto que seja sustentável no futuro. A descentralização do acesso à informação crítica de uma organização implica uma maior exposição aos riscos cibernéticos, pelo que será natural que se assista igualmente a um maior investimento e foco das organizações nesta área."

PAULO ESCARIGO
Diretor da Área de Sistemas de Informação da CA Seguros

"Na CA Seguros temos vindo a acompanhar com especial atenção o crescimento deste tipo de riscos. Temos vindo a apostar continuamente em medidas de proteção, nomeadamente através do ajuste das políticas de segurança, em especial nos dispositivos móveis. Paralelamente recorremos a auditorias externas com o objetivo de confirmar e validar os controlos existentes e detetar eventuais vulnerabilidades. No caso de verificarmos que nos encontramos demasiado expostos, então implementamos as medidas que nos são sugeridas de forma a reduzirmos o risco realizando internamente reavaliações periódicas. Como reforço da nossa proteção subscrevemos uma apólice de Seguro de Riscos Cibernéticos. O risco cibernético está a crescer, tendo o número de ciberataques triplicado na última década num momento em que estamos cada vez mais dependentes dos serviços digitais. O alvo preferencial dos ciberataques continua a ser o sector bancário, bem como respetivos clientes que utilizam os seus serviços digitais. Por outro lado, com a pandemia Covid-19 as empresas viram-se obrigadas a reforçar a sua aposta no digital e consequentemente ficaram mais expostas aos riscos cibernéticos. Como em todas as empresas a pandemia levou a uma reorganização interna e na CA Seguros foram criadas condições para os colaboradores realizarem as suas tarefas em regime de teletrabalho. Procedemos a melhorias significativas nas aplicações de Callcenter e de Callback, que muito agrado teve por parte dos nossos Clientes. Disponibilizámos acessos remotos à informação de forma segura e tornou-se normal a utilização de plataformas de videoconferência. Temos apostado ainda na automatização e integração de processos operacionais, com ganhos de produtividade e eficiência, através da implementação de *robotic process automation* (RPA). Lançámos no início do ano um conjunto de melhorias na App CA Seguros, uma aplicação que permite aos clientes consultarem as suas apólices e documentos, simular e subscrever seguros, alterar dados pessoais, pedir assistência, participar sinistros, marcar consultas médicas presenciais ou por videochamada, solicitar médico e medicamentos ao domicílio, entre outros."

PEDRO PINHAL
Diretor Técnico e Sinistros da MDS Portugal

"A indústria seguradora atua no âmbito do risco, pelo que necessita de acompanhar com especial atenção o desenvolvimento do fenómeno do risco cibernético. A MDS, enquanto consultora de risco e seguros dos seus clientes, desde há muito que tem equipas dedicadas e especialistas no âmbito do seguro *cyber*. Inovámos e fomos o primeiro *player* do sector segurador em Portugal a ministrar formação e a criar uma solução para ajudar as empresas a protegerem-se em face ao risco cibernético, ainda em 2015. O risco cibernético está em rápido crescimento, mutação e não tem fronteiras, pelo que se torna essencial um acompanhamento permanente da sua evolução e das ameaças existentes, adequando de forma contínua a proteção dos clientes. Por essa razão, disponibilizamos soluções de transferência de risco flexíveis e contruídas à medida das necessidades de cada cliente, de forma aumentar a sua resiliência e garantirem a continuidade das suas operações e atividades. É de salientar que o seguro cibernético não substitui nem exclui os mecanismos de segurança e os planos eficazes de resposta a incidentes; tal como estes também não tornam o seguro desnecessário ou redundante. O seguro e os mecanismos de segurança complementam-se. Aliás, é já um facto indiscutível que a maioria dos incidentes resulta, por variadíssimas razões e formas, do erro humano e não, unicamente, de problemas na infraestrutura de segurança. Por exemplo, a simples perda de um portátil ou de um telemóvel ou o descarregar, por descuido, de um ficheiro malicioso anexo a um email de *phishing* são erros humanos que abrem as portas dos sistemas aos *cyber* criminosos. O próprio seguro tem acompanhado a alteração das necessidades de mercado e evoluído para responder, eficazmente, às necessidades dos segurados e ser capaz de reduzir, com significado, o impacto económico e operacional de incidentes. Por outro, o impacto do atual surto pandémico na digitalização foi – e está a ser – absolutamente extraordinário. Se é certo que o processo de transformação digital já era uma realidade, com a crise sanitária provocada pelo Covid sofreu uma intensificação vertiginosa, tanto na velocidade, com a antecipação de medidas, como também no universo, já que o fenómeno foi transversal a praticamente todos os sectores da economia e da sociedade. A necessidade de reduzirmos a exposição ao risco de contágio e combater a propagação do vírus alterou, de um momento para o outro, a forma como trabalhamos, como adquirimos bens e serviços, e como comunicamos tanto a nível pessoal como profissional. E mudou as rotinas diárias de todos - famílias, alunos e empresas -, empurrando-as para um mundo virtual e tornando-as fortemente dependentes de sistemas informáticos, de redes *wifi* domésticas, de ferramentas de comunicação digital e de trabalho remoto. Este novo paradigma potenciou a exposição a riscos e vulnerabilidades no que à segurança cibernética diz respeito. Por um lado, pelo aumento dos possíveis alvos gerado pela proliferação dos pontos de acesso e, por outro, pelo incremento das fragilidades de segurança cibernética decorrentes da transição/transformação digital muito acelerada e pragmática, por vezes pouco planeada. A dimensão do risco cibernético está umbilicalmente ligada à digitalização, no sentido que quanto maior é esta também maior será o risco em termos de frequência e severidade."

NELSON FERREIRA
Financial Lines Manager da AIG Europe

"Muitas seguradoras, principalmente as mais pequenas, estão as sair do mercado de *cyber* e quase todas a reduzirem a capacidade (capital seguro) que estão dispostas a oferecer ao mercado. Esta dinâmica de menor oferta e maior procura tem levado ao aumento dos prémios, sendo uma tendência que se irá manter em 2021. Ora, isso também se irá reflectir no mercado português. Apesar de Portugal ser ainda um mercado pouco "maduro" no que diz respeito aos seguros *cyber*, algumas tendências dos mercados internacionais já se refletem no nosso mercado. As seguradoras e *brokers* terão que preparar bem mais os seus clientes para estas novas circunstâncias. Será necessário seguramente mais tempo de análise, assim como, exemplificar aos clientes os riscos e danos que o mundo cibernético podem trazer. E claro as soluções do mercado segurador, que são muitas e cada vez mais relevantes na política de gestão de risco das empresas. Mais importante, na minha opinião, é que este assunto não deve ficar apenas na responsabilidade de um Director Informático, mas sim também e, principalmente, com o CEO, porque o risco cibernético afeta várias áreas da empresa. E sem dúvida que o risco está a crescer e nenhuma indústria é imune a este risco. Obviamente empresas com marcas de maior notoriedade têm maior exposição."

ANTÓNIO CORREIA
Sales Manager da WatchGuard Portugal

O ciberrisco é uma nova área em Portugal, a dar os primeiros passos no portefólio das seguradoras, mas creio que, dado o potencial danoso das ciberameaças dos dias de hoje – especialmente sublinhado nesta era Covid – é um mercado em crescimento exponencial. O risco está a crescer a um ritmo alucinante, quer em quantidade, quer na sofisticação das ameaças. As empresas tendem a investir mais na prevenção de falhas e menos em estratégias desenhadas para detetar e antever futuros ataques. É, por isso, essencial prevenir, detetar e responder a qualquer tipo de ciberameaças. A segurança deve estar presente como elemento fundamental desde o início e deve ser entendida como um processo – não um estado imóvel. Por outro, o local de trabalho das empresas passou a ser composto por dezenas de funcionários espalhados pelas suas casas, em regime de teletrabalho, com a pandemia a forçar milhares de organizações portuguesas e no mundo a tornar o trabalho remoto o seu modus operandi, no espaço de algumas semanas. Embora muitas empresas se tenham preparado, algumas cederam portáteis configurados à pressa ou *desktops* que não foram inicialmente desenhados para sair da segurança da rede local, o que elevou exponencialmente a sua exposição a ciberameaças. Mesmo quando esta crise terminar, iremos perceber que este fenómeno provavelmente elevou o perfil do planeamento da continuidade de negócio para todas as organizações e que é extremamente importante consciencializar as forças de trabalho das empresas para as principais ameaças de segurança que podem afetar organizações de todos os tamanhos, mesmo quando estão fora do perímetro da rede da empresa, preservando ao mesmo tempo a sua produtividade."

MARCOS OLIVEIRA
Cyber Specialist do departamento de Broking & Specialties da Aon Portugal

"O risco cibernético tem evoluído drasticamente ao longo dos últimos anos, o que tem levado a uma adaptação constante do mercado para dar resposta às necessidades das organizações. De facto, o seguro *cyber* começou por se concentrar nas violações de dados, sendo que, hoje em dia, as organizações procuram seguros cibernéticos para fornecer uma cobertura completa mais holística das suas necessidades. Na Aon temos procurado encontrar/construir soluções que respondam às diferentes necessidades das organizações. É nosso entendimento que, para as pequenas e médias empresas cuja maturidade é limitada e em que os recursos financeiros não permitem grandes investimentos nesta área, a solução passa pela contratação de um seguro que incida fundamentalmente na prevenção e na resposta imediata a incidentes, através de um conjunto de serviços pré-incidente que permitam mitigar as debilidades e insuficiências, bem como na criação de planos de contingência e de resposta a incidentes. Este seguro é iminentemente propedêutico, permitindo a estas instituições ter um conjunto de parceiros especialistas na área, que farão evoluir positivamente a forma como a mesma lida com o risco. Por outro lado, para empresas de maior dimensão, cuja maturidade relativa é elevada e cujo investimento em segurança é considerável, deixa de se justificar a contratação de um seguro com este tipo de valências. Para este tipo de instituições, torna-se mais relevante, ter uma solução direcionada para um conjunto de coberturas pós-incidente, quer ao nível da resposta imediata a ataque cibernético quer a nível da responsabilidade civil e danos próprios, onde se destacam coberturas como "perdas de exploração", "Ransomware", "danos reputacionais" e "despesas legais". E, devido à pandemia que se abateu sobre o mundo, situação catastrófica que ninguém previu, verificou-se um aumento exponencial da utilização da internet para fins como o trabalho remoto, comércio online e comunicação pessoal e profissional. Para além do impacto óbvio relacionado com as questões humanas e sanitárias, há que ressalvar também o crescimento exponencial dos crimes cibernéticos, claramente relacionado com a utilização massiva da rede por pessoas sem experiência, atuando em ambientes corporativos ainda sem a devida implementação de um sistema de segurança de informação."

PUB

panda
a WatchGuard brand

WatchGuard

Um passo gigante para uma segurança integrada

Segurança de Endpoints

Segurança de Redes

Wi-Fi seguras na Cloud

Autenticação multifatorial

TELEFONE: 210 414 400

www.watchguard.com | pandasecurity.com

Acerca da WatchGuard Technologies:A WatchGuard® Technologies, Inc. é líder global na área das soluções de segurança de rede, das Wi-Fi seguras, da autenticação multi-fator e da proteção avançada de endpoints. Os produtos e serviços premiados da empresa contam com a confiança de organizações de todo o mundo, nomeadamente 10 mil revendedores de soluções de segurança e service providers, que, em conjunto, protegem mais de 80 mil clientes. A missão da empresa é tornar a segurança empresarial acessível às organizações de todos os tipos e tamanhos através da simplicidade, tornando a WatchGuard a solução ideal para PMEs e empresas distribuídas e PMEs. Com sede em Seattle, Washington, a WatchGuard tem escritórios na América do Norte, Europa, Ásia Pacífico e América Latina. Para mais informação, visite WatchGuard.com. Part No. WGCE67407_110620.