05

© Nicolau

Awareness key to cyber risk transfer demand

Consciencialização do risco cibernético: essencial para a procura de soluções de transferência

Mark Camillo of AIG discusses the development of the cyber insurance market in the US and Europe and believes that regulatory intervention and rising awareness can only help accelerate appreciation of and purchase of ever-improving insurance solutions.

Mark Camillo, da AIG, fala sobre o desenvolvimento do mercado de seguros contra riscos cibernéticos nos EUA e na Europa, e afirma acreditar que uma intervenção regulatória e um esforço de consciencialização viriam acelerar a valorização e a compra de soluções de seguros cada vez melhores.

Cyber risks continue to dominate the headlines, and organisations are increasingly aware of their potential liabilities either from attacks or from system failures. In recent research undertaken by AIG, 86% of those asked (including risk managers, brokers and C-suite executives) said they were "very" or "somewhat" concerned about cyber risk.

However, while the historic focus in the cyber market has been around the consequences of the loss of data, this is now shifting to network interruption.

Businesses increasingly rely upon external and internal communications networks to operate their businesses. If an attack means that the network is disrupted or out of commission for periods of time, then businesses suffer financial loss, as well as reputational damage.

So, how big is the issue and how is the insurance industry looking to solve this problem?

A real and present danger

According to recent reports, the number of detected cyberattacks skyrocketed in 2014, up 48 percent from 2013. The expected number of attacks is expected to surge to 42.8 million or roughly 117,339 attacks each day according to consulting firm PWC.

From a claims perspective, AIG is receiving notice of two incidents per business day on average. The types of incident range widely both in cause and in their location, but some recent examples include:

1. A company was undertaking work to upgrade its systems when it experienced a failure. The system took eight hours to restore fully, denying customers' access and causing considerable client dissatisfaction and reputational damage;
2. A hacker exploited a weakness in the insured's legacy web-facing systems and used this as a stepping stone to the internal network. As a result of the breach, the hacker was able to exfiltrate personal data. Significant costs were incurred to carry out the forensic analysis to resolve the problem. Legal and PR advice was also needed to deal with the fall-out;
3. A business received a ransom that demanded payment of a set sum or else their website would crash. The ransom was not made and as a consequence a denial of service attack was launched. As a result, the website crashed multiple times and, during just one of the attacks, the insured lost revenue that reached £250,000.

For most businesses, it is not a question of "if" but "when", and the landscape continues to evolve. For example, looking to the future, we expect to see an increase in cyber extortion claims as criminals seek more ways to monetize their exploits.

In addition, the rise of the "internet of things" and the reliance on third party Cloud providers means that a host of devices connected to the internet are now exposed to new types of risk, and so this could increase the number of interruptions.

Os riscos cibernéticos continuam a dominar as notícias, e as organizações estão cada vez mais conscientes dos potenciais prejuízos decorrentes de ataques ou de falhas do sistema. Numa recente investigação conduzida pela AIG, 86% dos inquiridos (incluindo gestores de risco, corretores e executivos de topo) afirmaram estar «muito» ou «de alguma forma» preocupados com os riscos cibernéticos. No entanto, embora historicamente o enfoque do mercado cibernético se tenha centrado nas consequências da perda de dados, começa hoje a transferir-se para a interrupção de rede.

As empresas baseiam cada vez mais as suas atividades em redes de comunicação e, se um ataque significar a perturbação ou a interrupção prolongada da rede, as empresas sofrem perdas financeiras bem como danos de reputação. Interessa, pois, conhecer a dimensão do problema e saber como está o setor dos seguros a procurar resolvê-lo.

Um perigo real e atual

De acordo com relatórios recentes, o número de ataques cibernéticos detetados subiu em flecha em 2014 – mais 48% do que em 2013 – e, segundo a empresa de consultoria PWC, o número de ataques deverá ascender a 42,8 milhões [em 2015] ou aproximadamente 117 339 por dia.

No que respeita a sinistros, a AIG está a receber em média duas participações por dia útil. Os tipos de incidente são muito diversos quer no que respeita às causas quer aos locais, mas entre os exemplos recentes contam-se os seguintes:

1. Uma empresa estava a atualizar os seus sistemas quando ocorreu uma falha. O sistema demorou oito horas a restabelecer-se por completo, negando o acesso dos clientes e provocando-lhes grande descontentamento, assim como danos de reputação à empresa;
2. Um pirata informático explorou uma debilidade num antigo sistema de acesso via Web de um segurado, tendo usado este sistema como porta de entrada para a rede interna. Em resultado desta quebra, o pirata conseguiu extrair dados pessoais. A empresa incorreu em custos significativos para levar a cabo a análise forense com vista à resolução do problema, bem como no aconselhamento jurídico e de relações públicas necessário para lidar com os efeitos colaterais;
3. Uma empresa recebeu um pedido de resgate exigindo o pagamento de um determinado montante sob ameaça de quebra do respetivo sítio Web. O pagamento não foi efetuado e, como consequência, foi lançado um ataque de negação de serviço. Como resultado, o sítio Web foi abaixo várias vezes e, só durante um dos ataques, o segurado perdeu receitas no total de 250 000 libras.

Para a maioria das empresas, não é uma questão de *se* mas de *quando* e o panorama continua a evoluir. Por exemplo, olhando para o futuro, esperamos ver um

A way forward

High profile incidents, occurring with seemingly greater frequency, are undoubtedly driving demand for cyber insurance.

Despite this, many organisations are still in the dark about possible solutions. One of the key problems is the level of knowledge and understanding.

There are still a significant number of businesses that are not even aware that cyber insurance exists. Amongst those that do, a large number are uncertain about what and how much to purchase as they struggle to assess their cyber-related exposures.

Cyber insurance has, so far, mainly covered data breaches pay outs for notification costs, experts to control the damage, costs of credit and ID monitoring, investigation costs, third party liabilities and regulatory investigations along with payment card industry fines and penalties.

However, more and more buyers seek to expand their coverage to include network interruption.

These extensions specifically cover the income loss from systems failure either from security failures, attacks or viruses. They can also be broadened to cover systems failure that might have come about internally such as through the failure of a patch.

The other area of concern that can be protected is the exposure to the unavailability of Cloud services. An increasing number of firms use off-site services (often with third party providers) and so there is a real need for contingent business interruption cover.

There are some interesting regional differences in the purchase of network interruption cover between the US and Europe.

Whereas less than 20% of AIG CyberEdge policyholders in the US opt for network interruption coverage, over 70% of EMEA clients select this option. This appears to be driven by the difference in regulatory regimes between the two geographies.

In the US, the states' requirement for the notification of data breaches means that US clients are more aware of the potential costs and liabilities that arise from the attacks. They are therefore more aware of the need for insurance.

In the EU, the proposed reform to the Data Protection Directive is taking time to take shape, and as a result, businesses are more focused on their business interruption exposures for now. In many cases they are only buying relatively low limits so far. But as their experience grows, undoubtedly so will the limits they require.

There can be no doubt that cyber liability is an matter that no organisation can afford to ignore, and now is the time to be thinking about what exposures business really face, both in terms of cost and consequence.

A better understanding of this will undoubtedly encourage businesses to buy a cyber policy and encourage further development by insurance providers. The solution lies in risk managers working together with brokers and underwriters to understand and articulate the company's risk profile so that they can find the best cyber protection program available in the marketplace.

aumento das queixas por ciberextorsão à medida que os criminosos procuram mais formas de rentabilizar as suas "proezas".

Além disso, o crescimento da «Internet das coisas» e a confiança em fornecedores externos de *Cloud* faz com que um conjunto de dispositivos ligados à Internet esteja agora exposto a novos tipos de risco, o que poderá aumentar o número de interrupções.

Mark Camillo
AIG – HEAD OF CYBER, EMEA

Mark Camillo is Head of Cyber, EMEA and is responsible for the CyberEdge® suite of end-to--end risk management solutions at AIG. Prior to this role, Mark led the cyber team for the Americas including oversight of the Personal Identity Coverage (PIC) and Payment Fraud Products.
Mark joined AIG in 2001 and has held positions of increasing management responsibility in various parts of the organization including eBusiness Risk Solutions, Affinity Group, Accident & Health, Professional Liability, and the Fidelity team. Prior to AIG, Mark worked in sales, marketing, and product development for Dun & Bradstreet (D&B) and SITEL Corporation. Mark has a Masters of Business Administration from SUNY Buffalo and a Bachelor of Science degree from the University of Wyoming.

Mark Camillo lidera a área de riscos Cyber da AIG para a região da Europa, Médio Oriente e Ásia e é responsável pelo CyberEdge®, um conjunto de soluções de gestão de riscos Cyber disponibilizado pela AIG. Anteriormente liderou a equipa de Riscos Cyber para o continente americano, incluindo a supervisão das áreas de proteção dos dados de identificação pessoal (PIC) e de proteção contra fraudes em matéria de pagamentos. Mark Camillo ingressou no Grupo AIG em 2001 e, desde então, tem vindo a assumir posições de crescente responsabilidade na gestão de várias áreas da organização, incluindo soluções para riscos no comércio eletrónico, grupos de afinidade, seguros de acidentes e de saúde, seguros de responsabilidade profissional e de fidelidade. Antes de ingressar no grupo AIG, Mark Camillo desempenhou funções nas áreas de vendas, marketing e desenvolvimento de produtos na Dun & Bradstreet (D&B) e na SITEL. Mark Camillo possui um Mestrado em Administração de Empresas (MBA) pela Universidade Estatal de Nova Iorque – Buffalo, e uma licenciatura em Ciências pela Universidade de Wyoming.

Um caminho a seguir

Os incidentes de grande repercussão, que aparentemente estão a ocorrer com maior frequência, estão claramente a incentivar a procura de seguros contra riscos cibernéticos.

Ainda assim, muitas organizações continuam "às escuras" no que respeita a possíveis soluções e uma das questões centrais está relacionada com o grau de conhecimento e de compreensão desta matéria.

Há ainda um grande número de empresas que ignora que existem seguros contra riscos cibernéticos, e entre as que conhecem a existência destes seguros, um grande número tem dúvidas sobre o que comprar e por que valor, uma vez que têm dificuldade em avaliar a sua exposição aos perigos relacionados com a Internet. Até à data, o ciberseguro tem vindo a cobrir sobretudo violação de dados, pagando os custos de notificação, especialistas para controlar os danos, custos de crédito e monitorização de dados pessoais, custos de investigação, responsabilidade civil perante terceiros, bem como as multas e as penalizações no setor dos cartões de pagamento.

No entanto, os compradores procuram cada vez mais alargar a cobertura de modo a que esta inclua a interrupção de redes.

Estas extensões cobrem especificamente a perda de rendimento decorrente de falhas de sistemas, seja por falhas de segurança, ataques ou vírus, mas podem ser alargadas para cobrir falhas de sistemas que podem ter origem interna – por exemplo, um *patch* que tenha falhado.

A outra área crítica que pode ser protegida é a da exposição à indisponibilidade de serviços de *Cloud*. À medida que o número de empresas que utilizam serviços remotos aumenta (muitas vezes recorrendo a serviços externos), existe uma necessidade real de cobertura da perda de receitas por interrupção da atividade.

Existem algumas diferenças interessantes na aquisição da cobertura de interrupção de rede entre a Europa e os EUA.

Enquanto menos de 20% dos tomadores de seguros CyberEdge da AIG nos EUA optam pela cobertura de interrupção de rede, mais de 70% dos clientes da zona EMEA (Europa, Médio Oriente e África) elegem esta opção. Este ato deve-se à diferença de regimes regulamentares entre estas duas geografias.

Nos EUA, o requisito de notificação de fugas de dados estabelecido pelos estados significa que os clientes norte-americanos estão mais cientes dos potenciais custos e responsabilidades decorrentes deste problema e, logo, da necessidade de seguro.

Na UE, a proposta de reforma da Diretiva de Proteção de Dados está a demorar a tomar forma, pelo que, por agora, as empresas estão mais centradas na interrupção das respetivas atividades. Em muitos casos, estão apenas a comprar limites relativamente baixos até ao momento, mas à medida que a experiência aumenta o mesmo acontecerá com os limites que exigem.

Não pode haver dúvidas de que a responsabilidade cibernética é uma questão que nenhuma organização se pode permitir ignorar e este é o momento para refletir sobre a exposição a que as empresas estão sujeitas – quer no que respeita a custos quer a consequências.

Um melhor entendimento deste ponto irá impreterivelmente levar as empresas a comprar apólices cibernéticas e motivar um maior desenvolvimento das mesmas por parte dos seguradores. A solução encontra-se no trabalho conjunto de corretores e subscritores por forma a compreenderem e articularem o perfil de risco de cada empresa para que esta possa obter o melhor programa de proteção cibernética disponível no mercado.