# 04 "To Boldly Go"..... Avançar com coragem.....

© Nicolau

**Geoff Kinsella**, Chief Operating Officer and Partner at Safeonline LLP, the specialist Lloyd's broker, urges business managers to take cyber risk seriously and to proactively protect their companies from the growing threat to their digital assets.

**Geoff Kinsella**, Diretor de Operações e Sócio da Safeonline LLP, corretor do Lloyd's especialista em seguros cibernéticos, recomenda aos gestores das empresas que tomem em séria consideração a ameaça do risco cibernético, e as protejam de forma proativa do crescente perigo a que os ativos digitais estão sujeitos.

Sendo fã de *O Caminho das Estrelas* (*Star Trek*) na infância, fiquei triste ao saber recentemente da morte do ator Leonard Nimoy que interpretava Mr. Spock na série. Ficava maravilhado com a forma como a tripulação era capaz de comunicar através de dispositivos portáteis, como eles eram capazes de falar com a imagem de alguém num ecrã, e como conseguiam recolher dados utilizando um *scanner*. Tudo coisas verdadeiramente 'inacreditáveis' que, no mundo 'livre de tecnologia' dos anos 60, pareciam tão futuristas.

No entanto, em 2015, muitas dessas 'invenções improváveis' são agora comuns. Comunicamos através de telemóveis. Armazenamos e recolhemos dados em dispositivos portáteis. Conduzimos a nossa vida *on-line*. Sabia, por exemplo, que o utilizador comum da Internet passa cerca de quatro horas e meia por dia a navegar na rede e que em 2014 os utilizadores de dispositivos móveis ultrapassavam 50% da população mundial?

As a Star Trek fan as a child, I was saddened recently to learn of the death of actor Leonard Nimoy who played Mr. Spock in the series. I marvelled at the way the crew could communicate with hand held devices, how they could speak to an image of someone on a screen, and how they could collect data using a scanner. All truly 'unbelievable' things that, in the 'technological' free world of the 60s, all seemed so futuristic.

In 2015 however, many of these 'improbable inventions' are now common place. We communicate with mobile phones. We store and collect data on handheld devices. We conduct our lives online. Did you know for example, that the average internet user spends around four and half hours using the net each day and that mobile device users exceeded 50% of the world population in 2014?

Businesses are becoming more and more virtual and the nature and the sheer volume of the data that we collect is growing exponentially.

Amazing isn't it? But as our reliance on technology grows, so do the risks that we face. Sadly, the more sophisticated that the technology becomes, so too do the cyber-criminals.

Cyber security now represents one of the biggest risks to the business community. Unlike other threats such as terrorism or natural disasters that are relatively 'area centric' events, a cyber related incident has no respect for geographical, political, cultural or natural boundaries. A major incident could affect organisations, or indeed national infrastructures, around the globe simultaneously. Also the perpetrator is most likely located thousands of miles from the scene of the crime.

State-sponsored cyber-attacks appear to be more overt as governments seek to gather sensitive information on their counterparts. Cyber extortion, hacktivism and cyber terrorism are now real threats and the number of incidents are growing.

49 percent of respondents in a recent survey said that they used their personal smart device for work and play. And 34 percent admitted using work devices for accessing their social network.

Is it any wonder therefore that "social engineer" attacks within organisations are also on the rise? Whether this involves tricking employees into unwittingly divulging sensitive information or using the employee as an unsuspecting 'accomplice' to plant malware into an organisation's system, organisations are finding it more and more difficult to protect themselves from an incident of this nature.

Unfortunately, the adage of 'it is not a case of if, but when' seems to hold true when it comes to the potential of a cyber related incident to your business.

When Safeonline was first founded in 1998 there were very few underwriters, brokers, or even clients interested in the cyber risk class. Thankfully this is no longer the case as the issue of cyber security is fast finding its way into the world's boardrooms and the insurance market responds creatively and effectively to this nascent risk class.

The improvement in education and understanding of digital risk within the corporate community, coupled

As empresas estão a tornar-se cada vez mais virtuais e a natureza e o volume dos dados que recolhemos está a crescer exponencialmente.

Surpreendente, não é? Mas, quanto mais aumenta a nossa dependência da tecnologia, aumentam também os riscos que enfrentamos. Infelizmente, se a tecnologia se torna cada vez mais sofisticada, o mesmo acontece com os cibercriminosos.

A segurança cibernética representa atualmente um dos maiores riscos para a comunidade empresarial. Contrariamente a outras ameaças, como o terrorismo ou os desastres naturais que são eventos maioritariamente 'locais', um incidente relacionado com a cibernética ignora fronteiras geográficas, políticas, culturais ou naturais. Um grave incidente pode afetar organizações, ou mesmo infraestruturas nacionais simultaneamente em todo o mundo. Além disso, o autor encontra-se muito provavelmente a milhares de quilómetros da cena do crime.

Os ataques cibernéticos conduzidos pelos Estados parecem ser mais evidentes à medida que os governos procuram obter informações confidenciais sobre os seus homólogos. Extorsão cibernética, *hacktivismo* e terrorismo cibernético constituem hoje ameaças reais, e o número de incidentes está a aumentar.

Num inquérito realizado recentemente, 49% dos inquiridos afirmaram que utilizam *smartphones* ou *tablets* para trabalhar e nos momentos de lazer. E 34% admitiram utilizar dispositivos de trabalho para aceder às redes sociais.

Será então de admirar que os ataques de "engenharia social" estejam também a aumentar no interior das organizações? Se isto implica induzir os colaboradores a divulgar inadvertidamente informações confidenciais ou utilizá-los como 'cúmplices' incautos para instalar *malware* no sistema de uma organização, as organizações estão a ter cada vez mais dificuldade em proteger-se de um incidente desta natureza.

Infelizmente, a questão não reside em saber "se", mas "quando", o que parece fazer todo o sentido quanto ao potencial de um incidente cibernético relacionado com o seu negócio.

Quando a Safeonline foi fundada em 1998, havia muito poucos subscritores, corretores, ou mesmo clientes interessados no risco cibernético. Felizmente a situação alterou-se, uma vez que a questão da segurança cibernética está a entrar rapidamente nos conselhos de administração das empresas e o mercado dos seguros está a responder de forma criativa e eficaz a este risco emergente.

Uma maior educação e compreensão acerca do risco digital no contexto da comunidade empresarial, aliada ao facto de haver uma maior disponibilidade de soluções de seguro abrangentes, levam a que não haja qualquer motivo para que uma organização não estar preparada para o risco digital. Se a tudo isto acrescentarmos o panorama legislativo em constante mudança e tendo este uma influência cada vez maior sobre a governação em matéria de segurança, torna-se claro que chegou o momento de as empresas começarem a agir.

O clausulado das apólices está em constante evolução por forma a oferecer coberturas mais abrangentes.

**Geoff Kinsella**
**CHIEF OPERATING OFFICER**
**PARTNER, ACTING ON BEHALF OF SAFEONLINE LLP, LLOYD'S BROKERS**

During his career, which spans over 35 years in the insurance arena, Geoff has worked in a variety of insurance/reinsurance markets including Ireland, Middle East, Canada and the UK Geoff has travelled extensively and has conducted insurance business on every continent (except Antarctica!). Geoff has held senior positions in a variety of Public and Private insurance entities.
Proving the adage that 'you can teach an old dog new tricks', Geoff turned his attention in 2012 to the emerging insurance market for Cyber risks and joined Safeonline in London as a Partner in 2013. Safeonline is a recognised leader in the provision of Cyber and Technology insurances and has developed a portfolio of proprietary products in this space. Geoff and his colleagues place and manage cyber risk insurances on behalf of a diverse range of clients within the Retail, IT, Energy, Entertainment, Hospitality, Healthcare, Public and Financial Services sectors.
Geoff is FCII qualified, a Chartered Insurance Practitioner & holds an MBA.

Ao longo de uma carreira de 35 anos na área dos seguros, Geoff Kinsella trabalhou em vários mercados de seguros e resseguro, incluindo a Irlanda, o Médio Oriente, o Canadá e o Reino Unido. Viajou por todo o mundo e realizou negócios de seguros nos cinco continentes (exceto Antártida).
Ocupou cargos de responsabilidade em diversas entidades seguradoras públicas e privadas. Contrariando o provérbio «burro velho não aprende línguas», Geoff focou-se nos mercados emergentes do risco cibernético, e, em 2012, tornou-se sócio da Safeonline em Londres.
A Safeonline é, reconhecidamente, a empresa líder na criação de soluções de seguros para riscos cibernéticos e tecnológicos, e desenvolveu uma carteira de produtos patenteados nestas áreas. Geoff e os colegas colocam e gerem seguros contra o risco cibernético em nome de uma grande variedade de clientes dos setores do retalho, das tecnologias de informação, da energia, do entretenimento, da hotelaria, e dos serviços públicos e financeiros.
Geoff Kinsella é membro acreditado do Chartered Insurance Institute na categoria de Practitioner da mesma instituição, e tem um grau de mestre em administração de empresas.

with the fact that comprehensive insurance solutions are now readily available, means there is no reason why any organisation should be unprepared for digital risk. Add to the mix the changing legislative landscape, which is having an ever-increasing influence on security governance, and it is clear that companies should act now.

Policy wordings are continually evolving to offer more comprehensive coverage. The sub-limits that used to abound are being replaced by the offer of full policy limits for areas such as crisis management expenses, customer notification expenses, payment card industry fines and credit monitoring expenses. Capacity has also increased, with a multitude of markets now active in this class. Solutions are now readily available for cyber-extortion and also for cyber--terrorism where none existed previously. Third-party vendors are also now being covered, with protection also being offered for cloud-based service providers. Losses that used to be commonly excluded under standard property and business interruption policies for cyber related physical and non-physical damage are now available.

If you have not done so yet, I would recommend speaking to your insurance adviser about cyber insurance products. We are all 100 percent reliant on our IT systems and we should proactively seek to mitigate the loss of this critical asset.

As Mr. Spock says, may you all "live long and prosper" as a result!

Os sublimites que eram habituais estão a ser substituídos por uma oferta em que coberturas como as despesas de gestão de crises, as despesas de notificação de clientes, as coimas aplicadas ao setor de cartões de pagamento e as despesas de monitorização de crédito, estão abrangidas pelo capital total da apólice. A capacidade também aumentou, com uma grande quantidade de mercados ativos no momento. Também nos dias de hoje, estão mais facilmente disponíveis soluções para fazer face à ciberextorsão e ao ciberterrorismo, soluções que anteriormente eram inexistentes. Existe também uma oferta de proteção para fornecedores subcontratados, bem como para fornecedores de serviços baseados na *cloud*. Está também disponível uma cobertura para prejuízos que eram comummente excluídos das apólices tradicionais de seguros patrimoniais e de perda para danos materiais e imateriais de natureza cibernética.

Se ainda o não tiver feito, gostaria de recomendar que se aconselhe com o seu consultor de seguros sobre produtos de seguros contra riscos cibernéticos. Estamos hoje inteiramente dependentes dos nossos sistemas de TI e devemos procurar pró-ativamente atenuar os danos associados a este ativo essencial.

Como resultado, e tal como diz Mr. Spock, "may you all live long and prosper"!