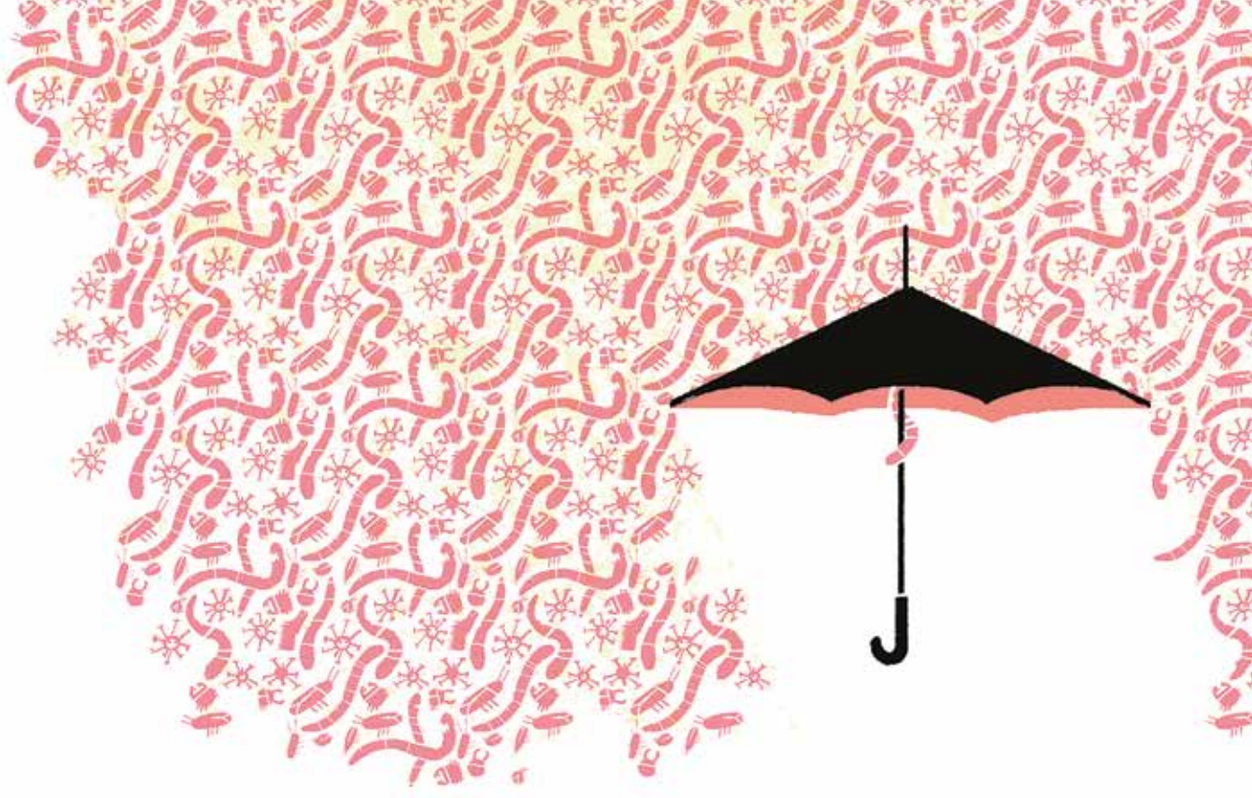
02



© Nicolau

A recipe for cyber defence

Uma receita para a ciberdefesa

Scott Corzine, Managing Director, Risk Management Practice, FTI Consulting, Inc., recently wrote an in-depth report on the management of cyber risk, focused particularly on the risk management requirements for insurance companies that hold huge amounts of customer data. Following is a summary of the reports key findings. The full report can be found on brokerslink.com/press.

Scott Corzine, Managing Director, Risk Management Practice, FTI Consulting, Inc., escreveu recentemente um relatório aprofundado sobre a gestão do risco cibernético, centrado sobretudo nos requisitos de gestão do risco das companhias de seguros que detêm grandes volumes de dados dos seus clientes. Em seguida apresenta-se um resumo das principais conclusões deste relatório. O relatório pode ser encontrado na íntegra em brokerslink.com/press.

As seguradoras, que têm grandes repositórios de informação pessoal identificável (IPI) de elevado valor, são cada vez mais alvo de ameaça de ataques cibernéticos. Estes ataques poderiam ter um enorme impacto, afetando não apenas os seguradores, mas também os segurados, e até alastrar às cadeias de abastecimento dos clientes. No recente relatório que elaborou sobre esta área crítica, Scott Corzine, afirmou que os potenciais danos decorrentes destas ameaças têm vindo a ser destacados em virtude do impacto de ataques recentes a grandes empresas de diferentes setores bem como a diversas agências governamentais dos EUA. «Estes ataques têm o potencial de perturbar a gestão, colocar relações valiosas em risco, levar a rescisões laborais e influenciar governos», indicou Corzine.

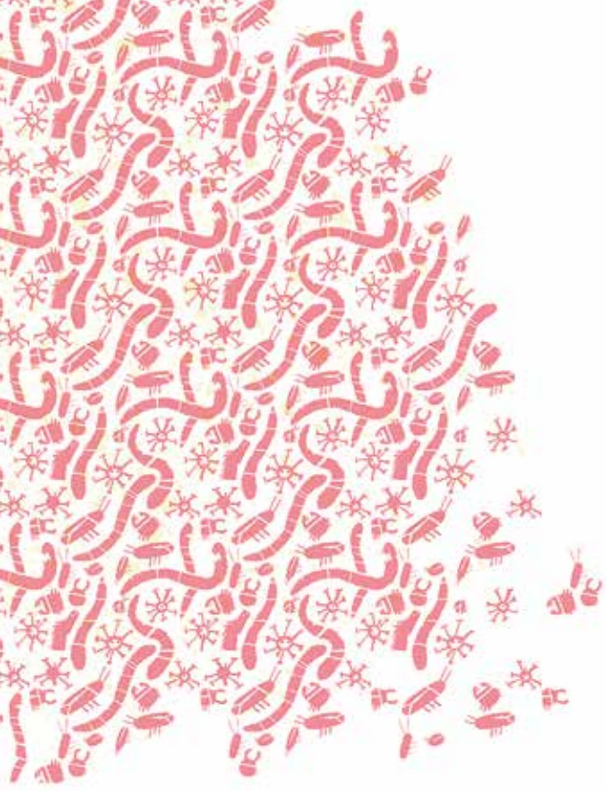
À medida que assistimos a uma escalada da frequência e da gravidade dos ciberataques de alto nível, os governos federais e estaduais dos EUA impõem regulamentação que exige que as organizações demonstrem uma melhor preparação e resiliência em caso de ataque cibernético.

Ao mesmo tempo, os meios de comunicação estão a contribuir para um aumento da consciencialização do público para este problema e as organizações de cibersegurança estão a fornecer ferramentas e metodologias melhoradas que podem ajudar as empresas a cumprir os requisitos de cibersegurança que lhes são impostos. Trata-se de uma área de risco e de gestão de risco em franco crescimento.

Corzine salientou que, neste contexto, é claro que as empresas têm de gerir a exposição aos riscos cibernéticos mais proativamente para ir ao encontro das exigências da nova regulamentação e, ao mesmo tempo, proteger a atividade, os clientes e a reputação da empresa.

Os piratas ou a espionagem *on-line* apoiados por estados podem dominar os títulos dos jornais, mas é importante ter consciência de que uma parte significativa das quebras de segurança cibernética se dão a partir do interior das organizações, destacou o especialista.

De acordo com o organismo sem fins lucrativos Online Trust Alliance, nos primeiros seis meses de 2014, apenas 40% das quebras de segurança que acarretaram a perda



Insurance carriers, with their large repositories of high-value personally identifiable information (PII), are increasingly threatened by cyber--attacks. Such attacks could have an immense impact, affecting not only the carriers, but also their insureds, and even ripple through to customer supply chains. In his recent report on this critical area, Scott Corzine said that the potential damage from such threats is underscored by the impact of recent attacks on large companies in numerous sectors as well as a US government agency. “Such attacks have the potential to embarrass management, place valuable relationships at risk, result in employment terminations, and influence governments,” pointed out Mr Corzine.

As the frequency and severity of high-profile cyber-attacks escalate, Federal and State government in the US are imposing regulations that require organisations to demonstrate better preparedness and resilience in the event of a cyber-attack.

At the same time, the media is increasing public awareness and cyber-security organisations are providing improved tools and methodologies that can help companies meet their cyber-security requirements. This is a fast-growing area of risk and risk management.

Mr Corzine stressed that in this environment, companies clearly need to manage their cyber risks more proactively to meet the requirements of the new rules and regulations and, at the same time, protect their business, customers and reputations.

Hackers or state-backed online espionage may grab the headlines but it is important to be aware of the fact that a significant portion of cyber security breaches occur from inside the organization, stressed the expert.

The non-profit body Online Trust Alliance recently reported that for the first six months of 2014, only 40% of data breaches that involved the loss of PII were caused by external intrusions. Some 29% were caused either accidentally or maliciously by employees, it found.

de informação pessoal identificável (IPI) foram provocadas por interferências externas. Cerca de 29% tiveram causa acidental ou deveram-se à intervenção mal-intencionada de funcionários, verificou este organismo.

A Online Trust Alliance apontou a falta de controlo interno, o roubo e a perda de dispositivos e documentos, bem como a engenharia social e a fraude como os principais fatores causadores de quebras de segurança. No mais recente estudo «Law and Boardroom Study» da *Corporate Board Member/FTI Consulting, Inc.*, aproximadamente 50% dos administradores e consultores jurídicos apontaram a «segurança dos dados» como a sua principal preocupação em termos jurídicos e de gestão do risco. À medida que o risco aumenta, os reguladores estão a alargar o âmbito das suas exigências de cibersegurança bem como de imposição do respetivo cumprimento.

«Os reguladores estão cada vez mais a atribuir aos seguradores a responsabilidade pelas suas próprias medidas de cibersegurança de forma a proteger melhor os tomadores de seguro», escreveu Corzine.

«Os seguradores guardam dados importantes que são potencialmente desejados por cibercriminosos. A dependência de parceiros e prestadores de serviços externos expõe os seguradores a vulnerabilidades adicionais do ponto de vista cibernético provocadas por estas entidades subcontratadas», acrescentou.

Como era de prever, os reguladores estão a começar a impor melhorias na segurança cibernética através de novas regras que exigem aos seguradores a implementação de programas abrangentes de cibersegurança.

A National Association of Insurance Commissioners (NAIC — Associação Nacional de Comissários de Seguros), por exemplo, afirmou em janeiro passado, que planeia propor orientações para as entidades que avaliam as práticas de gestão de risco das seguradoras.

A Direção de Proteção e Programas Nacionais do Departamento de Segurança Nacional dos Estados Unidos da América discutiu também com o setor dos seguros a criação de um repositório de dados de incidentes cibernéticos por forma a que se constitua um depósito de dados atuariais de riscos cibernéticos e das análises das consequências destes incidentes, necessário para fazer crescer o mercado dos seguros de cibersegurança. O Departamento de Serviços Financeiros de Nova Iorque anunciou, em dezembro último, que tomará medidas para ajudar os seguradores estaduais a reforçar as defesas de cibersegurança e irá dar início a avaliações para determinar o grau de preparação e cumprimento das mesmas.

Praticamente todos estes instrumentos regulatórios, em constante desenvolvimento, estabelecem prazos específicos para a prestação de informação sobre fugas de dados às autoridades e aos clientes afetados e penalizações explícitas pela omissão desta informação, afirma Corzine.

As organizações de segurança como a ISO e a ISACA estão também a intensificar os esforços nestas áreas.

«No esforço que desenvolvem para conseguirem reforçar a resiliência da segurança cibernética, os seguradores têm uma dupla responsabilidade: têm de se preocupar com a cibersegurança da sua própria organização bem como com a cibersegurança dos segurados», afirma Corzine.

SCOTT CORZINE
MANAGING DIRECTOR AND CO-LEADER OF THE RISK MANAGEMENT PRACTICE AT FTI CONSULTING

Scott Corzine is a Managing Director and Co-Leader of the Risk Management Practice at FTI Consulting, a global consulting firm with a specialty in the insurance sector. He is responsible for providing risk mitigation and resilience services – business continuity, IT disaster recovery, crisis management, and information security assessment and planning – to public and private sector clients globally. Scott was a co-founder of Risk Solutions International (RSI) which was acquired by FTI Consulting in 2013. He has been part of Brokerslink for a number of years, and has spearheaded initiatives in business continuity planning for airports globally, visibility into contingent business interruption in the supply chain, and business continuity solutions to help mitigate supply chain resilience risk. Scott is passionate about providing these services to Brokerslink members to help improve their competitive advantage in broking transactions.

Scott Corzine é Diretor Executivo e co-Líder da área de Gestão de Risco na FTI Consulting, uma empresa global de consultoria com uma especialização no setor segurador. É responsável pela prestação de serviços de mitigação de risco e resiliência, bem como de continuidade de negócio, recuperação em caso de desastres de TI, gestão de crise e avaliação e planeamento de segurança da informação, a clientes dos setores público e privado em todo o mundo. É cofundador da Risk Solutions International (RSI), empresa adquirida pela FTI Consulting em 2013. Integrado na Brokerslink há vários anos, Corzine tem liderado várias iniciativas nas áreas de continuidade de negócio, seja para a actividade de aeroportos em todo o mundo, seja para mitigação do risco de "supply chain", nomeadamente no que respeita à perda de receita. Nutre uma paixão pelo trabalho que desenvolve na Brokerslink, disponibilizando estes serviços aos seus membros, por forma a que possam melhorar a sua vantagem competitiva nas operações de corretagem.

© Nicolau

The Online Trust Alliance cited lack of internal controls, lost or stolen devices and documents, as well as social engineering and fraud as the main factors.

In the most recent Corporate Board Member/ FTI Consulting, Inc. *Law and Boardroom Study,* approximately 50% of polled directors and general counsels named 'data security' as their number one legal and risk management concern.

As the risk rises, regulators are expanding the scope of their cyber security requirements as well as compliance enforcement.

"Regulators are increasingly holding insurers accountable for their own internal cyber-security measures in order to better protect policyholders," wrote Mr Corzine.

"Insurers maintain significant data that is potentially desirable for cyber thieves. Dependence on outside partners and third party service providers additionally opens insurers to the cyber-vulnerabilities of these outsourced contractors," he added.

Predictably, regulators are starting to compel improvements in cyber security through new rules that require insurers to implement comprehensive cyber security programs.

The National Association of Insurance Commissioners (NAIC) stated in January, for example, that it plans to propose guidance for insurance examiners who review companies' risk management practices for cyber security risks.

The Department of Homeland Security's National Protection and Programs Directorate has also discussed a cyber-incident data repository with the insurance industry to create a warehouse of cyber risk "actuarial data and consequence-oriented analytics" that is needed to grow the cyber security insurance market.

New York State Department of Financial Services announced last December that it will take measures that help in-state insurers strengthen their cyber security defenses and will begin assessments to determine the degree of preparedness and compliance.

Virtually all of these evolving regulations have specific deadlines for the reporting of data breaches to authorities and affected customers, and explicit penalties for non-disclosure, said Mr Corzine.

Security organisations such as ISO and ISACA are also stepping up their efforts in this areas too.

"In their quest to achieve cyber-security resilience, insurers have a dual responsibility – they must address the cyber security of their own organisation as well as the cyber security of the customers that they insure," stated Mr Corzine.

The author has identified seven key points that insurers should consider to help build a more robust and mature cyber security capability. These can be summarised as the following:

- View cyber security as an organisational issue, not simply as a technical issue. Management must take responsibility for this risk and not just leave it up to IT departments;
- Obtain access to trusted third party resources, partly to help tackle the internal threat;

O autor identificou sete pontos-chave que os seguradores deverão ter em atenção para construírem uma capacidade mais forte e amadurecida em termos de:

- Considerar a cibersegurança uma questão organizacional e não apenas uma questão técnica. A gestão tem de assumir a responsabilidade por este risco, não o relegando simplesmente para os departamentos de TI;
- Ter acesso a recursos externos fiáveis, em parte para ajudar a enfrentar a ameaça interna;
- Adotar doutrinas de governação e conformidade e estabelecer um quadro de gestão de risco que ajude a atingir os objetivos;
- Compreender e documentar o respetivo apetite pelo risco, ou seja, o nível de risco que a organização está disposta a aceitar para alcançar os seus objetivos empresariais antes de ter de tomar medidas para o reduzir;
- Levar a efeito uma avaliação de ameaças, vulnerabilidades e impacto. Esta análise deverá avaliar o valor da informação e o potencial impacto operacional e financeiro resultante de danos ou perdas de informação, bem como dar uma indicação sobre os passos necessários para a proteger. As avaliações deverão incluir uma análise da apólice de ciberseguro da organização para ajudar os decisores a perceberem se as coberturas são adequadas e se encontram efetivamente em linha com os restantes riscos cibernéticos da organização e se os limites, as retenções e as exclusões são apropriadas;
- Desenvolver programas e estratégias de mitigação do risco. O objetivo é decidir quais são as exposições, as vulnerabilidades e os riscos que exigem uma análise de custo-benefício, a alocação de recursos, financiamento e uma tomada de decisão, incluindo se se deverá recorrer ao autosseguro ou adquirir um seguro.
- Preparar um Plano de Resposta a Incidentes Cibernéticos (PRIC) que determine a forma como a organização responderá a uma fuga de dados de uma maneira planeada e eficaz. O PRIC é concebido para garantir que os incidentes relacionados com a segurança cibernética são geridos de forma a limitar o respetivo impacto, conquistar a confiança das partes interessadas na capacidade da organização para gerir incidentes e reduzir o tempo e o custo de recuperação. O PRIC deverá ser formalmente analisado e adotado pelo Conselho de Administração e levado a efeito pelo menos uma vez por ano.

"A adoção desta abordagem abrangente à gestão do risco cibernético deverá ajudar os seguradores a manter a viabilidade financeira e a manter a conformidade com as exigências regulamentares. Os seguradores deverão igualmente exigir que os seus cibersegurados sigam, de alguma forma, esta abordagem para promover uma cultura de consciência do risco, reduzir as possibilidades de falhas de segurança catastróficas e evitar o pagamento de reclamações de elevado valor que poderiam ter sido evitadas ou minimizadas", concluiu Corzine.

—

- Adhere to governance and compliance doctrines and establish a risk management framework to help accomplish program objectives;
- Understand and document your definition of risk appetite that is the level of risk that an organisation is willing to accept in order to achieve its business objectives before it needs to take measures to reduce the risk.
- Perform a threat, vulnerability and impact assessment. This analysis should work out the value of information, the potential operational and financial impact of impairment or loss of that information and provide guidance on steps needed to protect it. The assessments should include an examination of the organisation's cyber insurance policy to help decision makers understand if coverages are adequate and effectively aligned with the organization's remaining cyber risks, and if limits, retentions, and exclusions are appropriate.
- Develop mitigation programs and strategy. This should decide which exposures, vulnerabilities, and risks require a cost/benefit analysis, resource determination, funding, and decision-making, including whether to self-insure or purchase insurance.
- Prepare a Cyber Incident Response Plan (CIRP) that documents how the organisation will respond to a breach in a planned and effective way. The CIRP is designed to ensure that cyber-security incidents are managed in a way that limits impact, gains stakeholder confidence in the organization's capacity to handle incidents, and reduces the time and cost-to-recovery. The CIRP should be formally reviewed and adopted by the Board, and exercised at least once every year.

"Adopting this comprehensive approach to cyber risk management should help insurers sustain financial viability and meet regulatory compliance requirements. Insurers should likewise require some level of this approach from their cyber-insureds in order to promote a culture of risk awareness, reduce the chance of a disastrous breach, and avoid paying costly claims that could have been avoided or minimized," concluded Mr Corzine.

—