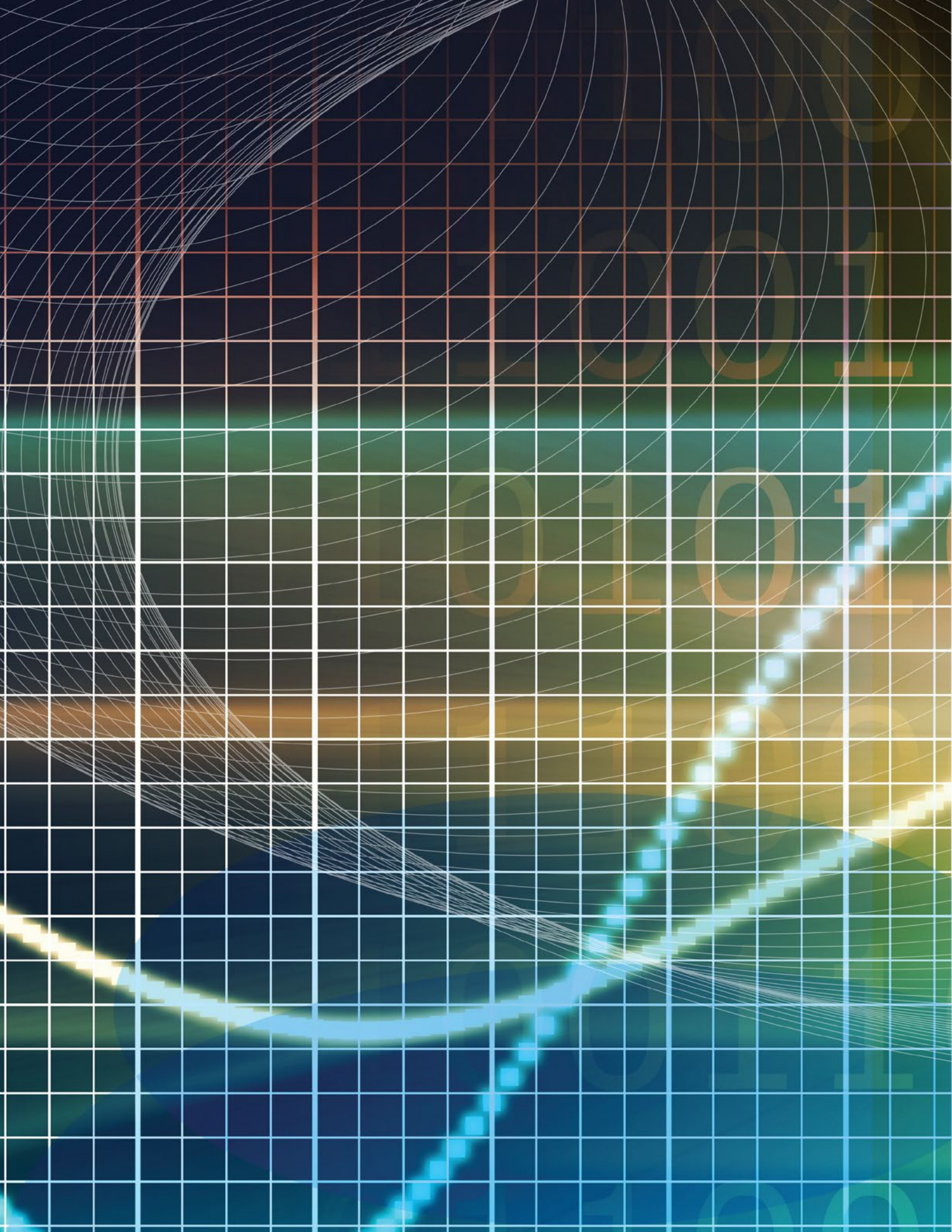

The Future of
Cyber Insurance
Crawford®



The Future of Cyber Insurance

In 2013, UK and Irish businesses alone sustained an average of more than 70 new infections a day, putting them both in the top 10 countries exposed to persistent threat. The cost to organisations of data breaches is growing and most of the consequential losses currently remain uninsured. One of the key challenges in aiding the development of a viable cyber insurance market is finding the right approach to handling both first and third elements of complex cyber claims, according to Benedict Burke, senior vice president, Crawford & Company.

Cyber attacks at well-known institutions and our growing reliance on technology have captured the attention of risk managers together with the tightening of data protection legislation. Cyber liability is identified in third place as the emerging risk likely to have the biggest financial impact on global organisations over the next two years, according to one recent survey.

Risk managers do not have to look far for examples of the impact a cyber attack can cause. Last year was the worst year to date for data breach with 740 million data files viewed or stolen around the world, according to Data Breach Today. The hacking of US retail giants Target and Neiman Marcus compromised the personal information of over 100 million customers. And in February, Europe and the US were hit by what is thought to be the largest-ever Denial of Service (DoS) attack directed at servers.

Beyond the immediate financial impact of recovering lost or damaged data, the cost of notifying customers and other stakeholders, the fines and penalties potentially levied by regulators and the lasting reputational harm a breach can cause mean that the $ value of a cyber attack is escalating. Take Sony PlayStation in 2011 was exposed in an estimated 77 million of its user accounts and although they estimated the cost of the breach to be in the region of $170m, some analysts pegged the overall impact (including loss of customers, drop in share price) at a significant multiple beyond this.

The nature of cyber attacks is also evolving. While the Target breach grabbed headlines, so-called "Point of Sale" attacks are old news, according to Verizon, which warns of a growth in attacks on websites. In today's interconnected world (think of the risk exposure in the telecommunications, technology and media sector as an example), an online crisis such as the failure of a major cloud provider could well be the next global "shock", according to a new Zurich report. "Cyber risks are not self-contained within individual enterprises, hence risk managers must expand their horizons," it warns.

Inadequate Insurance Response

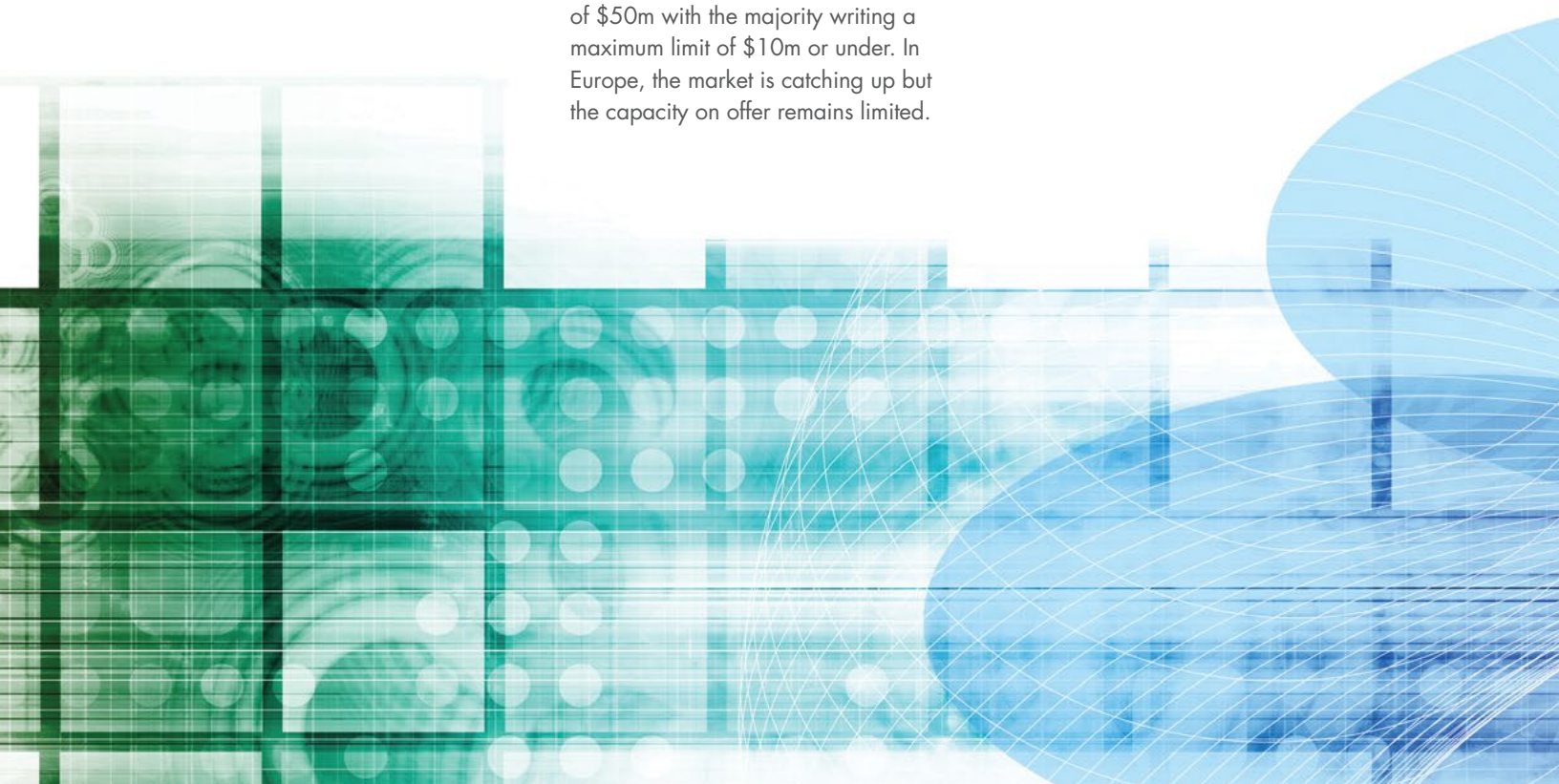
The insurance industry is at the relative infancy stage of responding to risk managers' concerns with bespoke cyber insurance products. However, current limits available in the Lloyd's and company market are low and attachment points high. Brokers are working better with insurers to expand wordings in existing classes such as GL, D&O, crime and product liability to encompass company's cyber exposures, but it is early days. Other brokers are creating specific cyber products and looking for market support both regionally and globally for their wordings.

At present many cyber losses involving digital attacks and data breach are uninsured. Insurers currently lack the data and claims history to build an accurate picture of the exposure and in lieu of this are reluctant to offer broad coverage wording and capacity to fully indemnify against first and third party cyber risks.

In the US where the market is most developed, annual gross written premiums are around $1.3bn, according to last year's Betterley Report. Very few carriers are able to offer indemnity in excess of $50m with the majority writing a maximum limit of $10m or under. In Europe, the market is catching up but the capacity on offer remains limited.

With such an unsubstantial commercial insurance market for cyber some insurance buyers are opting to put these liabilities through their captive insurer - if they have one - or simply retaining the risk on their own balance sheet. We anticipate this will change as the market develops, urged on by brokers requesting broader coverage terms and greater capacity and in part driven by changing legislation.

In March, the European Parliament voted in favour of new European Data Protection Regulation. The reforms include mandatory data breach notification (within 24 hours if feasible) and an increase in fines for failing to protect sensitive information to 5% of annual worldwide turnover (or EUR100m, whichever is greater). Whilst the legislative process has some way to go before an agreed text becomes law it is clear that when the rules come into place it will dramatically increase the exposure of European corporates, creating a more insistent need for risk transfer solutions, crisis management and loss value calculations and mitigation strategies.



Loss Calculation

One feature all cyber claims have in common is their high degree of complexity. It is the timely response to these complexities which can help minimise the overall impact of a network failure or data hack. A dialogue between risk managers, information officers, their brokers, insurers and claims professionals is essential in building a distinct methodology for coping with cyber claims. This is best done in advance of the breach; being part of an agreed approach to the loss / claims quantification methodology (CQM).

An effective response will encompass business continuity and third-party notification as well as crisis management and forensic IT investigations. As the standalone market for cyber insurance grows and as existing covers expand to encompass cyber exposures, we will see more and more claims come into the market. Involving claims experts with the capability to handle the inherent complexity of such losses will be a crucial step in convincing risk managers the industry is ready to offer a real solution.

Benedict Burke is senior vice president, global markets at Crawford & Company and Council member of the Chartered Institute of Loss Adjusters.

Benedict Burke BA ACII FCILA
Senior Vice President, Global Markets
Crawford & Company
T: +44 (0) 207 265 4041
M: +44 (0) 7919 552624
E: benedict.burke@crawco.co.uk
www.crawfordandcompany.com

The Seven Aggregations of Cyber Risk

	Description	Examples
Internal IT enterprise:	Risk associated with the cumulative set of an organization's (mostly internal) IT	Hardware; software; servers; and related people and processes
Counterparties and partners:	Risk from dependence on, or direct interconnection (usually non-contractual) with an outside organization	University research partnerships; relationship between competing/cooperating banks; corporate joint ventures; industry associations
Outsourced and contract:	Risk usually from a contractual relationship with external suppliers of services, HR, legal or IT and cloud provider	IT and cloud providers; HR, legal, accounting, and consultancy; contract manufacturing
Supply chain:	Both risks to supply chains for the IT sector and cyber risks to traditional supply chains and logistics	Exposure to a single country; counterfeit or tampered products; risks of disrupted supply chain
Disruptive technologies:	Risks from unseen effects of or disruptions either to or from new technologies, either those already existing but poorly understood, or those due soon	Internet of things; smart grid; embedded medical devices; driverless cars; the largely automatic digital economy
Upstream infrastructure:	Risks from disruptions to infrastructure relied on by economies and societies, especially electricity, financial systems, and telecommunications	Internet infrastructure like internet exchange points and submarine cables; some key companies and protocols used to run the internet (BGP and Domain Name System); internet governance
External shocks:	Risks from incidents outside the system, outside of the control of most organizations and likely to cascade	Major international conflicts; malware pandemic

[1]Emerging Risks Barometer: ACE European Risk Briefing 2013
[2]Beyond Data Breaches: Global Interconnections of Cyber Risk, Zurich 2014

Crawford®

BROADSPIRE®

CONTRACTOR CONNECTION™

EDUCATIONAL SERVICES

GLOBAL TECHNICAL SERVICES™

PROPERTY & CASUALTY

RISK SCIENCES GROUP®

SPECIALIST LIABILITY SERVICES™

STRATEGIC WARRANTY SERVICES™

Benedict Burke
Senior Vice President
Crawford & Company
T: +44 207 265 4000
M: +44 7919 552624
E: benedict.burke@crawco.co.uk

Clive Nicholls
Senior Vice President
Crawford & Company
T: +44 207 265 4000
M: +44 7802 591111
E: clive.nicholls@crawco.co.uk

www.crawfordandcompany.com

Crawford®

The Crawford Solution℠
The most comprehensive global solution for claims administration
NYSE: CRD-A, CRD-B | Crawford & Company
| 1001 Summit Blvd | Atlanta GA 30319 | 800-241-2541

CRAW-CYBER-BRO-A4-WP-0614