News release

Date	**14 Sept 2015**
Contact	Ellie Raven, Media Relations, PwC Tel: +44 (0) 207 804 3663, +44 (0) 7525 925 830 e-mail: ellie.raven@uk.pwc.com
Pages	2

Cyber insurance market set to reach $7.5 billion by 2020 – PwC report

The global cyber insurance market could grow to $5bn in annual premiums by 2018 and at least $7.5bn by the end of the decade, according to "Insurance 2020 & beyond: Reaping the dividends of cyber resilience", a new report issued by PwC at the Monte Carlo Reinsurance Rendez-vous today.

Previous PwC research revealed that 61% of business leaders across all industries see cyber attacks as a threat to the growth of their business, and 2014 saw an average of 100,000 global security incidents a day.

Paul Delbridge, insurance partner at PwC, said:

> "Given the high costs of coverage, the limits imposed, the tight terms and conditions and the restrictions on whether policyholders can claim, many policyholders are questioning whether their policies are delivering real value. There is also a real possibility that overly onerous terms and conditions could invite regulatory action or litigation against insurers.
>
> "As Boards become increasingly focused on the need for safeguards against the most damaging cyber attacks, insurers will find their clients questioning how much real value is offered in their current policies. If insurers continue to simply rely on tight blanket policy restrictions and conservative pricing strategies to cushion the uncertainty, they are at serious risk of missing this rare market opportunity to secure high margins in a soft market. If the industry takes too long to innovate, there is a real risk that a disruptor will move in and corner the market with aggressive pricing and more favourable terms."

PwC suggests that insurers, reinsurers and brokers can capitalise on the cyber risk opportunity whilst managing the exposures by:

- Maintaining their own cyber risk management credibility through effective in-house safeguards against cyber attacks

- Robustly modelling exposures and potential losses will provide a better understanding of the evolving threat and could encourage more reinsurance companies to enter the market:
  - Identifying concentrations of exposure and systemic risks in an increasingly inter-connected economy
  - Evaluating Probable Maximum Losses and extreme events/scenarios, and monitoring and modifying these regularly as new types of attack arise
  - Assessing and monitoring trends in frequencies and severities of attritional and large losses, and in the types of attack being perpetrated

- Partnering, sharing and coordinating:
  - Partnering with technology companies and intelligence agencies to develop a holistic and effective risk evaluation, screening and pricing process
  - Data sharing between insurance companies to secure greater pricing accuracy
  - Finding a risk facilitator (possibly the broker) to bring all parties (corporations, insurers, reinsurers, policymakers) together to coordinate risk management solutions, including global standards set for cyber insurance

- Making coverage conditional on a full and frequent assessment of policyholder vulnerabilities and agreement to follow agreed prevention and detection steps
  - this could include exercises that mimic attacks to highlight weaknesses and plan for responses

- Replacing annual renewals with real time analysis and rolling policy updates

Paul Delbridge, insurance partner at PwC, concluded:

"For insurers, cyber risk is in many ways a risk like no other. It is equally an opportunity. Insurers who wish to succeed will base their future coverage offerings on conditional regular risk assessments of client operations and the actions required in response to these reviews. A more informed approach will enable insurers to reduce uncertain exposures whilst offering clients the types of coverage and attractive premium rates they are beginning to ask for.

"Insurers also need to continue to invest appropriately in their own cyber security – a business which can't protect itself can't expect policyholders to trust them to protect and advise them. Given the huge volume of medical, financial and other sensitive information they hold, it is critical that insurers have closely monitored, highly effective cyber security frameworks in place. Sustaining credibility in the cyber risk market is crucial when looking to become a leader in this fast growing market. If this trust is compromised, and with innovative competitors knocking on the door, it would be extremely difficult to restore brand reputation."

Notes to editors

- "Insurance 2020 & beyond: Reaping the dividends of cyber resilience" can be found at the below link: http://pwc.to/cyber
- Paul Delbridge is available for interviews before and during the Monte Carlo Reinsurance Rendez-vous. Please contact Ellie Raven on +44 (0) 20 7 804 3663 or ellie.raven@uk.pwc.com for more information
- 1322 CEOs interviewed for PwC's 18th Annual Global CEO Survey revealed that 61% of business leaders across all industries see cyber attacks as a threat to the growth of their business (www.pwc.com/ceosurvey)
- PwC's annual survey of security, IT and business executives shows that there were nearly 43 million incidents in 2014. 'Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015", PwC

About PwC
PwC firms help organisations and individuals create the value they're looking for. We're a network of firms in 157 countries with more than 195,000 people who are committed to delivering quality in assurance, tax and advisory services. Find out more and tell us what matters to you by visiting us at www.pwc.com.

PwC refers to the PwC network and/or one or more of its member firms, each of which is a separate legal entity. Please see www.pwc.com/structure for further details.

©2015 PricewaterhouseCoopers. All rights reserved.