Subject: Insurance implications of cyber crime

Presenters	APPG	Others
Matt Cullen, Assistant Director, Head of Strategy, ABI Richard Bach, Assistant Director - Cyber Security, Information Economy, Department for Business, Innovation & Skills Carla Baker, Senior Manager, Government Affairs, Symantec Sarb Sembhi, Chairperson of the ISACA International GRA Committee Matt Webb, Head of Technology and Cyber at Hiscox UK	Jonathan Evans MP	Lord Erroll David Morey, PwC Jonathan Swift, Incisive Media Others – approximately 18 interested parties, representatives of the industry and trade press

1. Background

Cybercrime risk to business in the UK and globally is growing - 81% of large businesses and 60% of small business suffered a cyber security breach in the last year and the average cost of breaches has nearly doubled since 2013[1].

Jonathan Evans introduced the session by referring to the rapidly changing technology giving rise to new opportunities for insurance, and a need to maintain close dialogue between the market, the insurance sector, regulators and politicians. A key will be the need for affordable and fair insurance solutions for businesses impacted by new risks and the data revolution in progress where data security is key.

2. Presentations – key points

i) Matt Cullen, ABI

- We are experiencing a technological revolution which itself affects insurance pricing, insurance cover / products, marketing, claims and fraud prevention
- The rise of the "digital native" is changing the way society makes business and financial decisions. PwC have estimated that by 2019, digital natives will dominate business decisions.
- We are moving to a world of customer interactivity, personalisation and transparency, whereby customers can transact in real time on a variety of digital channels
- The insurance sector needs to keep pace and respond to these significant changes
- The volume and variety of cyber risks is increasing, but this also presents opportunities (e.g. autonomous vehicles, and access to assets rather than ownership of assets).

[1] 2014 Information Security Breaches Survey - http://www.pwc.co.uk/assets/pdf/cyber-security-2014- technical-report.pdf

ii) Richard Bach, BIS

- Cyber security is not new. But the threat comes in many guises – nation-states, hacktivists, investigative journalists and the public. Cybercrime is now worth more than the illicit drugs market

- Cybercrime tools are readily available on the internet – allowing users to develop a sophisticated cybercrime capability

- Insurance is not an alternative to cyber security, but it does allow transfer of some residual risks. Businesses need good underlying cyber security hygiene in any event

- The Cyber Essential Scheme helps business get the basics right, particularly in connection with the commonly used on-line cyber threats. This also includes a test mechanism to help users determine implementation

  [Cyber Essentials is a government-backed, industry supported scheme to help organisations protect themselves against common cyber attacks. The Scheme identifies five control themes (all of which need to be implemented in line with the requirements document and test specification), covering:
  1. Boundary firewalls and internet gateways
  2. Secure configuration
  3. Access control
  4. Malware protection
  5. Patch management.]

- Whilst Lloyd's sees cybercrime as an emerging market, the underlying risks are not new. However, the level of understanding of the risks still has some way to go, and the insurance sector's response to cybercrime still needs to mature.

- Marsh has established an initiative to help address some of the key challenges.

  [The membership of this initiative have committed to work together with Government to develop the cyber insurance offer. To deliver this offer, industry-chaired working groups will be established including representatives from Government. These working groups will explore how best to:
  - use insurance as a driver for improving cyber security practice in UK businesses, and SMEs in particular
  - model the impact of cyber attack scenarios on UK businesses and the insurance response
  - explore the possible role for the insurance industry in reducing the impact of cyber attack on critical national infrastructure.

  These groups will help contribute to a shared goal of driving growth in the effective use of cyber insurance and establishing the UK as the leading market for global business. The working groups will report emerging conclusions to the Cabinet Office by April 2015. Source: Cabinet Office statement].

iii) Sarb Sembhi, Security Advisory Group of ISACA

- Some of the underlying threats and risks have not changed significantly

- Typically regulatory action against firms has tended to be linked to where simple security errors have arisen e.g. lost discs

- Looking ahead, with the increasing use of smart technologies (e.g. driverless cars, smart TVs etc), which tend to be based on internet connectivity, there are new challenges albeit the older issues have not yet been resolved

- Increasingly, people's homes are being de- perimeterised with TVs, CCTVs, burglar alarms etc all using the same technologies which exhibit the same vulnerabilities

- Insurers will increasingly need to look at how insurance cover is constructed around people rather than necessarily their individual assets such as cars and contents. In addition, increasingly mandatory cover for cyber might be beneficial.

iv) Matt Webb, Hiscox UK

- Cyber insurance has been available since the mid to late nineties; the extent of cover is changing, but take up rates are typically low

- More recently, cyber risks are being better recognised albeit sophistication levels are typically low – in the US cyber insurance penetration rates are higher (circa 30%) than UK (circa 5%); insurance take up is increasing

- In the US, mandatory notifications of security breaches to customers and regulators acts as a stimulant to better awareness as well as a number of high profile data breaches

- In the UK the new EU General Data Protection Regulation in 2015 will bring in more obligations regarding lost data; this suggests a significant opportunity for insurers

- For insurers there is limited loss history (as there is with established catastrophe risk e.g. wind storm). It is necessary to look at single points of failure and the number of impacted customers to understand systemic risk

- Hiscox are a part of the Marsh initiative with Francis Maude, aiming to model cyber risks and the insurance response.

3. Q & A

Following the presentations, a number of points were discussed:

- Insurance is not a panacea – it will only provide cover where there is transfer of risk. Basic underlying cyber security remains a key priority for business

- London is a hub for cyber risk experts, and cyber security / insurance presents a significant market opportunity for London

- Inability to insure against Financial Conduct Authority fines (e.g. for data security breaches)

- Whilst we are seeing a revolution in connectivity and miniaturisation, it is based on internet engineering which is an open field of play for hackers. There is a need for pervasive and smart use of encryption. Insurers will typically exclude risks where minimum cyber security and encryption is absent

- There is a need for improved domestic security and encryption standards and usage

- There is also a need to standardise insurance definitions, as well as policy cover and pricing, regarding cyber – currently there is a significant variation in policy wordings. This reduces the level of confidence by buyers of insurance. ABI is looking at a good practice guide on wording definitions

- There is a significant opportunity to increase awareness of cyber risk and cyber security hygiene across smaller businesses (role for industry bodies, educational events etc). Insurers need to consider how cyber protection might be included in other covers to improve take up.

4. The Group's view

The Group supports the further development of cyber insurance but recognises this is only a partial solution, and that businesses need to engage with cyber security measures to mitigate many cyber risks. The Group will be interested to see the outputs from the working groups which will report emerging conclusions under the Marsh initiative to the Cabinet Office by April 2015.

David Morey
26 November 2014