‘Cyber Risks Insurance: the challenge and the opportunity’

A BAE Systems Detica Cyber Insurance briefing held in the Lloyd’s of London Library on Thursday 24 November 2011

This paper is an informal summary of a private Cyber briefing held on 24 November 2011 as part of Detica’s Security Horizons programme. The briefing discussions were held under the Chatham House rule. This paper is not a verbatim transcript of the discussion and does not necessarily reflect the views of any one person present at the briefing.

INTRODUCTION

Few areas of our lives remain untouched by the digital revolution. All organisations depend on the continuous availability, accuracy and confidentiality of information and networks. In the midst of this ongoing 'digital explosion', greater opportunities now exist for those with malign intent. Cyber security is rising ever higher on the board agenda of companies across the world, partly driven by recent high profile attacks.

As the profile of cyber risks has grown, so has interest in related insurance cover. But the risks are not well understood and the market for this type of cover is still in its infancy. So where do we go from here? At this executive seminar, organised by BAE Systems Detica, senior cyber insurance brokers and underwriters, selected insurance buyers from large UK corporations and relevant Government departments came together to discuss the challenge and the opportunity of cyber risk insurance.

Cyber insurance is a hot topic. Many people are talking about it…and many want to underwrite it. But dig a little deeper and the picture becomes less clear. What exactly is the risk? What should be insured, and are the right policies available to provide this cover, at a fair price?

We know that companies are struggling to measure and quantify the cyber risks that they face. The insurance industry can play a key role in helping to price this risk accurately. Insurers will need to build an empirical evidence base in order to price effectively and this will remain a challenge for as long as most incidents go unreported. We know from Cabinet Office research, carried out with Detica, that the overall cost to UK business of cyber crime is £21bn - largely due to industrial espionage and IP theft. Information sharing is key to combating the cyber threat, and until reporting rates increase, there will be no clear picture of the threat environment to help insurers calculate risk. Better risk quantification will lead to more appropriate levels of cyber defences and could drive the growth of a substantial new line of business for forward-thinking insurers.

This paper outlines key points from presentations and discussions which examined the challenge from four angles:

- Regulation can help to make markets. What is the evolving regulatory backdrop? What are the true costs of customer data loss and how can companies do a better job of valuing their information assets?
- Against this backdrop where is the demand for cyber insurance coming from? What products are available to meet this demand, and where does more need to be done?
- All good insurance markets are backed by an effective reinsurance market. The briefing covered a proposal for a cyber reinsurance vehicle with the aim of helping make the UK more attractive to IT-intensive businesses.
- Finally, the question of how to assess cyber risk effectively. During the discussion we examined two components of a long term solution – information sharing and the need for effective standards.

SECTION 1: Cyber risks and the evolving European regulatory framework

The US has led the way in Data breach notification law. First introduced in California in 2003 the regulation is now active in over 45 US states. The law requires an agency, person or business that conducts business in any of the relevant States and owns or licenses computerized 'personal information' to disclose any breach of security (to any resident whose unencrypted data is believed to have been disclosed). The specific requirements do vary somewhat from state to state.

In the EU the Data Protection Directive (95/46/EC) 'harmonises' the regulation of processing personal data in Europe. It contains a provision which requires companies to implement appropriate technical and organisational measures to protect personal data (Art. 17) but, importantly, contains no express duty to notify data subjects or regulators of any lapses in security. The situation is different for Telecoms providers however where there is now compulsory data breach notification.

It was also noted that entities regulated by the Financial Services Authority (FSA) are subject to specific guidance regarding data breach notification as set out in 'Data Security in Financial Services' (2008).

The existing EU Data Protection Directive (95/46/EC) is currently under review and Commissioner Reding announced in presenting to the British Bankers' Association on 20 June 2011: "I intend to introduce a mandatory requirement to notify data security breaches — the same as I did for telecoms and internet access when I was telecoms commissioner, but this time for all sectors, including banking and financial services".

Currently in the UK there is no legal obligation to report, although serious breaches should be reported to the individual and if there is a large number of people or serious consequences to the ICO. As at 4 August 2011 a total of 1893 data breaches had been reported to the ICO since November 2007 – 1205 from the Public sector, 605 from the Private sector. The remaining 83 breaches have been reported by Telecoms companies since 26 May 2011.

In the Ponemon Institute's 2010 Annual study: the UK cost of a data breach the average cost per record lost was estimated as being c. £72. In the same study the percentage of breach costs by cost activity was also assessed. 42% was attributed to lost customer business, 12% to investigations and forensics and 11% to notification costs.

Recommended legal solutions to the issue include:

- Review data protection and information security policies
- Review the disciplinary procedures for breach of policy
- Determine awareness of policies and introduce or update training
- Review your standard contracts, and key contracts with third party service providers
- Review your method of permitting the international transfer of personal data
- Review your PCI DSS position, if applicable
- Review your insurance position
- Develop a data breach response plan
- Consider adopting "International" standards – e.g. BS7799 / ISO 27001 / ISO 27002

SECTION 2: The Market Response

Many companies are asking 'where is our current cyber liability and exposure?' Often, it is found in two key areas:

- Network Security Liability: Denial of Service attacks, Transmission of malicious codes and Data breach (theft of data or unauthorised access or use);
- Privacy Liability: Your privacy policy (internal), your privacy notice (external), data you collect and data you share with others.

As part of assessing this risk, an organisation needs to understand whether it is a Data Owner, and the specific data that it owns (as opposed to processes on behalf of another Data Owner).

The types of exposure can be summarised into three categories:

- Liability: law suits from customers and Consumer class action suits;
- Regulatory: defence costs, privacy regulatory proceedings including fines and consumer redress;
- Privacy event expenses: notification costs, forensics, legal and PR, credit monitoring.

Data breach attracts a lot of media attention, but a company's exposure can be much broader than this. Organisations need to ask themselves some questions about how they operate:

- Business Practices:
  - Are you collecting post code information when you collect credit card payments?
  - Does your privacy policy reflect your current business practices? And if you change your business practices do you change your privacy policy and provide notice first?
- Privacy Policy:
  - Does your Privacy policy address core privacy principles such as Use & Retention, Disclosure and Monitoring & Enforcement as it relates to customer personal information?
- Technology:
  - Are your security controls reasonable and consistent with your industry peers?
  - Is your technology compliant under PCI (PA-DSS)?
- Web site:
  - Are you using tracking technologies on your web site, such as cookies and flash cookies, and are you disclosing them to your customers, including what is collected and who you share it with?

SECTION 3: The Cyber Insurance marketplace

So why do organisations consider transferring data Cyber risks through Cyber Insurance:

- Many functions are conducted by outside vendors and contractors who may lack insurance and assets to respond. What if the vendor makes a systemic mistake?
- No system can be designed to eliminate the potential for loss, as people and process failures cannot be eliminated. Insiders may be perpetrators.
- Responsibility rests with the data owner from a legal, regulatory perspective.
- There is potential for investor fallout from uncovered losses with large claim and class action, which could result in major impacts on your brand and reputation.
- Traditional P&C insurance does not cover Network Security liability or adequately address Privacy Liability.

The current cyber insurance market is immature; in particular it has:

- capacity of between $300 - $350 million;
- limited uniformity coverage or policy wording;
- to provide tailored insurance solutions based on an organisation's particular exposures.

Those insurers that offer data breach coverage have broadly adopted one of two different approaches:

- Indemnity coverage:
  - Reimbursement policies allow the insured to hire vendors (with consent from the carrier);

    - Some carriers recommend vendors who can manage a data breach response; others providing a risk transfer solution (e.g. reimbursement of privacy event expenses);
    - Privacy event expenses are typically subject to a sub-limit and erode the policy aggregate limit.

- Through Vendor Panels:
    - Automatic vendors provided by carriers;
    - Some carriers offer notification costs outside of the aggregate limit;
    - Some carriers offer notification costs per affected individual rather than monetary sub-limits.

Cyber liability coverage options include:

- Network Security Liability
- Media Liability
- Privacy Liability
- Privacy Regulatory Proceeding and Fines
- Technology Liability and Miscellaneous Professional Liability (Add-on)
- Privacy Event Expense Reimbursement
- Extortion Payments

Ist Party Cyber coverage options include:

- Data/Electronic Information Loss
- Business Interruption or Network Failure Expenses
- Cyber-extortion

All of these coverage options are subject to the earlier proviso – the market is immature with limited capacity for significant risks and a lack of uniformity of coverage.

SECTION 4: Cyber reinsurance – an enabler?

Summary

High-profile cyber-crimes on financial markets have led to significant losses. Cyber-crime insurance is a weak market where it is hard to get significant risks written. Market cover is sporadic above a handful of computers and fades completely above £100 million. Cyber-terrorism, insurance doesn't even exist. This market problem resembles terrorism for property insurance where the government created Pool Re to help in 1993. Why don't we have a Cyber Re where government helps the insurance industry fund extreme losses? As an example, government takes responsibility, via a reinsurance club, for risks at the highest levels. Below that level normal insurers write cyber policies which help spread information and best practice. With a fully functioning market, the UK would be more attractive to ICT businesses such as financial exchanges and large internet firms.

Background

This proposal was developed by Z/Yen, a commercial think tank. It originated with reactions and inactions to cyber-enabled thefts on the carbon trading markets associated with the European Trading System. In January 2011 over €45 million was stolen from the carbon markets. Carbon markets were closed on 19 January and have fitfully reopened since. The January 2011 attacks were preceded by attacks in 2009 and 2010. A 2 February 2010 phishing theft of 250,000 carbon emission permits was reported to net €3 million and also closed the markets.

Cyber-crime (e.g. "e-risk business protection") insurance typically covers crisis management costs, customer notification expenses, data extortion, professional services, multimedia liability (e.g. defamation, copyright infringement), security & privacy liability, and privacy

regulatory defence & penalties. Cyber-crime insurance is a weak market where it is hard to get significant risks written. Market cover is sporadic above a handful of computers (cyber equivalent of appliance insurance) and fades completely above £100 million.

Cyber-crime at scale is indistinguishable from cyber-terrorism. State actors may be involved. In fact, it is likely that only failed or corrupt states would allow attacks to originate from their territory. So firms are sensitive about the commitment of the state to protect them from incursions of substance, whatever the source. Cyber-terrorism insurance doesn't yet exist.

Currently insurers in the UK can reinsure liabilities from terrorism, in excess of the first £75m, with Pool Re. A member's retention is proportionate to their participation in the scheme. The only exclusions applying to the terrorism cover of Pool Re are in respect of: "war and related risks; and damage to computer systems caused by virus, hacking and similar actions."

Proposal

Why don't we have a Cyber Re (or extend Pool Re) where government helps the insurance industry fund the extreme losses of cyber-crime? As an example, government takes responsibility for risks above a point, say £100 million. Below that point normal insurers write cyber policies which help spread information and best practice and bear the risks up to £X million on any single incident or £Y million on combined incidents (X and Y might be numbers in the range of 50 to 100). Reinsurance helps form successful commercial insurance markets by providing assessable mutuality for random events. Cyber Re can increase supply by spreading large losses and, over time, playing a role in establishing a body of data to support more accurate pricing of the risk. It also helps demand by promoting an understanding of cyber risks and the value of defending against them.

Benefits

With a fully functioning market, the UK would be more attractive to ICT businesses such as financial exchanges and large internet firms. A few points of note emerge from the above:

- Cyber Re exists not to insure, but to allow insurers to insure by providing re-insurance, in turn providing regulators with the assurance that cyber insurance can be safely underwritten;
- Cyber Re is focused on creating a club with members, thus encouraging members to share information and reduce risk by sharing information with government, such as near misses, as well as to grow their market;
- Cyber Re should be quite small operationally and operate at close to no-cost.

Cyber Re can confer competitive advantage on the UK. The 10 April 1992 St Mary Axe bombing was a significant catalyst for Pool Re. As insurers refused to provide cover against acts of terror, financial services firms, noting what had happened to the Baltic Exchange, stated that they had troubles locating or expanding in London and the UK generally. With Cyber Re, the UK would have definite attractions to firms that depend on computers, particularly financial and internet firms, as it would be the only country that indemnifies should it fail to protect against cyber-crime at scale.

SECTION 5: Assessing your risk and understanding the threat

Cyber crime is a significant but poorly understood risk. It's sobering to realise that it is possible for an organisation to experience a very significant data breach without actually knowing about it…and there are many unreported incidents. Examples include:

- A global engineering organisation who invested $100million in a significant R&D project who then found critical designs had been stolen and taken outside their organisation.
- The McAfee 'Shady RAT' report in August 2011 which identified attacks on high-profile U.S. government agencies, the United Nations, the IOC, and numerous defence contractors. Many of those organisations involved had been compromised for over a year without knowing.

Awareness of the scale and sophistication of cyber attacks has improved dramatically over the last 12 months, although there is still some way to go. There are now encouraging signs that Board Directors and senior Security executives are getting a better feel of what is going on and what is critical to them to protect. In March 2011 the UK Cabinet Office published, 'The Cost of Cyber Crime' in conjunction with Detica. It is estimated that the cost to industry from Cyber Crime is £21million of which £17billion is estimated to result from Cyber Espionage.

More needs to be done to bring to light the true nature and scale of the cyber threat. Information sharing is key to this, and we are starting to see some encouraging signs regarding mechanisms to enable this.

The challenge remains that, in the UK, there is no significant incentive to report data breaches and other cyber attacks. Many organisations remain unaware of attacks to their IP or customer data and many are not looking. If there is no clear motivation for organisations to either look for or report incidents, the picture will remain incomplete at best..

Another significant challenge is that it is difficult for organisations to asses their risk and vulnerability to attack. Effectively, the challenge for any Board is to understand the answer to the question 'So how secure are we?' Standards could help with this, although it is important to recognise that there are gaps in the standards in use today. For example:

- There is great variability of maturity in the way organisations that adopt the same standards understand and mitigate against the risks they face. An interesting example is to see how two similar organisations who are both ISO27001 compliant respond to the same security threat:
    - The first hosts potentially sensitive data in a data warehouse accessible from the same machines that can also access the corporate network and internet;
    - The second hosts similar data on a separate network totally inaccessible from the corporate network and internet;
    - The result is that the first organisation is significantly more vulnerable to data breach despite having the same level of ISO compliance.
- The PCI DSS standard does contain sensible controls, though this has narrow applicability and the danger of specifying controls is that they can become outdated as cyber criminals identify means to circumvent them.

One possible answer could be to develop 'Objective Attack Standards' – defining standards for protecting against different 'Attack' threats rather than levels of 'Defence'. In other words an organisation could, based on an agreed set of clearly defined standards, invest to protect themselves against a attacks of different levels of sophistication. These could range from the general level of background virus and malware threat through to targeted, persistent and well funded attacks. This approach would allow organisations to adopt the defences that made sense in their particular context. It would also prevent the need to continually update standards to reflect the rapid advances in attacker 'tradecaft'. At the same time, it would allow any organisation to be easily able to decide and invest against which level of attack they are prepared to defend against.

SUMMARY

- It is clear that cyber risks are moving higher on the corporate agenda, and companies are beginning to look to insurance to deal with those aspects of the risk that they cannot manage themselves.

- The market does have some challenges today. Demand is patchy as the scale and nature of the risk is not yet widely understood. For similar reasons, insurers and reinsurers alike have concerns regarding their ability to price the risk accurately.

- The event heard three ideas that may help with these challenges.
    - The first was for a government-backed cyber reinsurance vehicle;
    - The second covered the need for greater information sharing to help companies and their insurers to understand the true nature and scale of cyber risks;

- The third proposal regards the need for standards to support rapid assessments of the vulnerability of individual organisations.

- All of these suggestions have merit and should be explored further as the market matures. For those organisations who are already actively writing cyber insurance, or who are considering entering the market, Detica can help in a number of ways today:

    - We can improve risk assessment – by deploying our experts to perform targeted assessments, embedding our knowledge into your underwriting process or deploying tools to help you extract insight from the unstructured data within and outside your organisation;

    - We can mitigate cyber risks – by providing managed security services and by undertaking specific organisational, process and/or technical initiatives to reduce an organisation's risk profile;

    - We can respond to incidents – our forensics capability can support the client response, or be used to support loss adjustment. We can also configure a full incident response service to enhance client service and increase the predictability of loss cost.

About BAE Systems Detica

BAE Systems Detica delivers information intelligence solutions to government and commercial customers. We help them collect, exploit and manage data so that they deliver critical business services more effrectivelyand economically. We also develop solutions to strengthen national security and resilience.

We integrate and deliver world-class solutions to our customers' most complex operational problems – often applying our own unique intellectual property. Our services include cyber security, managing risk and compliance, data analytics, systems integration and managed services, strategy and business change and the development of innovative software and hardware technologies.

Detica is part of BAE Systems, a global defence and security company with over 100,000 employees worldwide.

For more information contact:

BAE Systems Detica
Surrey Research Park
Guildford
Surrey GU2 7YP

Tel: +44 (0)1483 816000
Email: queries@baesystemsdetica.com