AIG CyberEdge

Cyber: Joined up?

Findings from independent research among senior business leaders at the UK's largest companies, suggest more needs to be done to increase awareness of the vulnerabilities and consequences in relation to cyber risks. We believe greater joined-up thinking and board engagement is necessary.

Much has been written about the cyber threat in the last few years in the media, with the breadth of risks faced by almost every business. The landscape continues to evolve rapidly, prompted by greater dependence on the cyber world, economically and socially (as demonstrated by developments such as the Internet of Things). This increased reliance on the internet and technology has, unfortunately, come hand in hand with more frequent, sophisticated and professional cyber-crimes. While the question businesses used to ask was 'will I be targeted?', now it is more likely to be 'when?'

Originally focussed on data loss/ breach, potential triggers and impacts have widened to include business interruption, theft of IP and even inter-connected events such as bodily injury and physical damage with liability implications. Furthermore, the global economy is becoming increasingly networked, with disruption due to cyber threats more likely to lead to financial and reputational damage. Cyber risk has therefore moved from being an IT risk to an enterprise-wide risk management issue that needs attention at board level; a top-tier emerging risk for both businesses and their directors.

With UK government involvement and the upcoming EU cyber security directive, cyber risk is also taking centre stage. The government has recognised cyber attacks to be one of the most significant risks facing the UK, with the cost to businesses rising. For larger companies, the first step towards improving their cyber risk framework is to ensure that their standard cyber 'hygiene' is properly addressed (the NIST in the US provides detailed benchmarking via its Cyber Security Framework). For SMEs, in 2014 the government launched the Cyber Essentials scheme to help guide businesses in protecting themselves against cyber threats.

With attacks increasing and implications becoming more far-reaching, companies need to actively reduce their exposure to being targeted. And, if they are targeted, consider how they can reduce the impact and mitigate their risk in the future. Having an action plan in place prior to an event is critical, as are end-to-end solutions involving consultation leading to extra layers of prevention.

Insurance plays a key role in not just offsetting costs when an event happens, but preventing an attack in the first place, and responding correctly to mitigate when cybersecurity does fail. The underwriting process helps different parts of a company unify and focus on what their vulnerabilities are and where they can work together to mitigate them.

In response, the global cyber insurance market is growing significantly at around 25-30% per year and has a value of around $1.5-2bn.

AIG conducted this research to understand the views of senior business leaders at very large companies – an exclusive audience typically very hard to access. While we know through other research that 88% of FTSE 350 companies include cyber risk within their strategic risk report, there is little published data on deeper perspectives. The findings can also be used as a reference point to compare to the future attitudes and behaviour of mid-sized and smaller companies as the cyber market matures further.

> Cyber risk has moved from being an IT risk to an enterprise-wide risk management issue

Key Themes

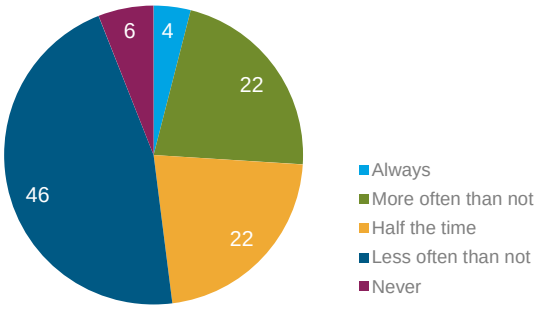
We see four key themes emerge.

1. **Cyber security needs to be given greater prominence at board level**

   While 82% of senior business leaders stated they know either a great deal or a fair amount about their company's cyber security governance and risk management framework, their cyber security policy is not discussed regularly at board meetings. Board involvement in how the organisation protects itself is critical.

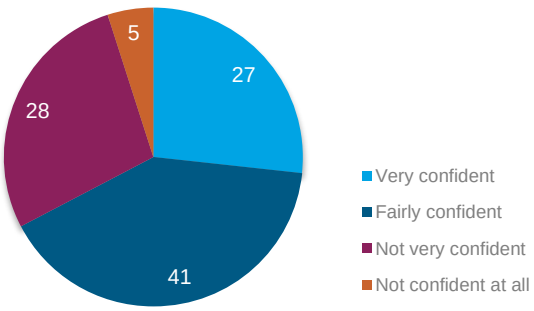
   Only just over a quarter of companies (26%) discussed their cyber security policy regularly (defined as always or more often than not), while over half (52%) discussed rarely i.e. less often than not, or never (Chart 1).

Chart 1: Thinking about board meetings in the last twelve months, how often have you discussed the company's Cyber Security Policy?



Base: British Captains of Industry [108]

Chart 2: How confident are you that directors fully understand the legal implications of a serious cyber security breach?



Base: British Captains of Industry [108]

This context may link to the fact that companies are split as to whether the maintenance of cyber security levels is designated at board level. The board has overall responsibility in 9% of companies, with a key board member having ownership in a further 43% - making a total of just over half (51%) of companies having strong board representation. Certainly, having key roles in place like a Chief Information Security Officer, who reports to the CEO, is considered best practice.

However over a third (36%) of companies mention their IT department as being designated for the maintenance of cyber security, and with a further 11% of 'other' responses it is noticeable that almost half (47%) do not designate cyber security to be a boardroom issue. What we have learned from large breaches, is that cyber security risk is not just a technology issue. It takes an enterprise-wide effort to prevent attacks and to mitigate damage when they happen. While the day-to-day responsibility may rest with the technical or security teams, strategy and response needs to have ownership across functions, hence the need for board engagement.

So, how confident is the board on emerging cyber threats? While there is undoubtedly confidence among many companies, with three quarters (77%) feeling confident, a substantial minority of nearly a quarter (23%) are not very confident or not confident at all on the board being up to date on the nature of cyber threats in this area of rapid change.

2. **While many directors may understand the financial consequences of a breach, there is a knowledge gap about the legal implications**

   Much has been written in the media about the financial consequences of a cyber event – whether a regulatory fine from a data breach, or other material remediation required. This research confirms that directors in these large companies are generally confident in their understanding of the financial consequences of a serious cyber security breach, with 86% feeling very or fairly confident and only 13% not feeling confident about the implications. This is a key priority, since the cost of dealing with a data breach continues to rise.

   However, when asked about their understanding of the legal implications of a serious security breach, almost a third (32%) say they are not very or not at all confident, while 68% say they are confident (Chart 2). This is concerning, given that boards and management can be held accountable for this significant business risk. In the UK, directors could potentially be liable if their failure to prepare for cyber events constitutes a breach of their duty to the company. In the US, shareholder lawsuits have been filed against boards following large scale data breaches.

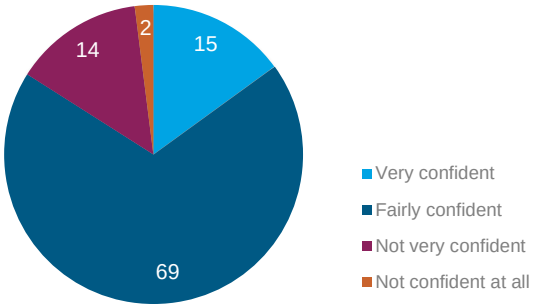
3. The high level of stated confidence in companies' IT departments may be misplaced

Overall, companies feel that they have identified their levels of vulnerability across all key information assets in relation to their company's governance and risk management of cyber security. A total of 90% feel very or fairly confident in their identification, with only 10% not feeling confident.

Furthermore, a very significant 84% think that their IT department is able to protect the company from a cyber attack. Only 16% are not confident in this regard (Chart 3).

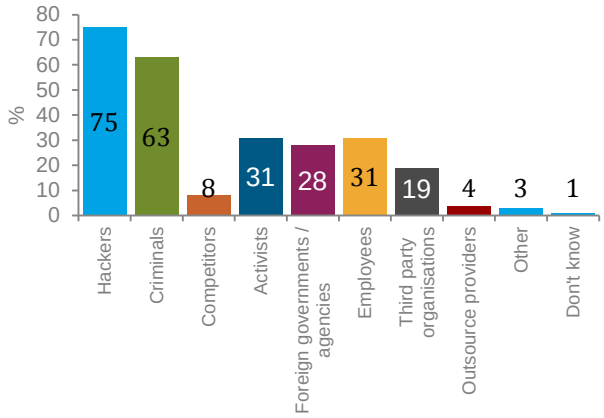
Perhaps this confidence is grounded in the fact that 45% of companies surveyed have experienced a cyber security breach. However, with 62% thinking it likely that their company will be the subject of a cyber attack in the next 12 months and the potential impacts of an attack becoming more serious, there is no room for complacency. There is a problem in relying solely on the IT department for data protection risk management in that no set of controls can guarantee a data breach won't happen. In fact, following a serious cyber event, one of the first casualties is often the head of IT. Specific questions can gauge the maturity of a company's cyber security program, to understand if cyber security is taken seriously at every level of the company, including the board room.

Chart 3: How confident are you that the IT department is able to protect the company from a cyber-attack?



Base: British Captains of Industry [108]

Chart 4: From where do you feel cyber attacks against your company are most likely to originate?



Base: British Captains of Industry [108]

4. While hackers and criminals may represent the greatest perceived threat to cyber security, problems internal to the organisation caused by employees cause a significant number of breach cases

Senior business leaders believe that cyber attacks against their company come from a number of sources. Hackers and criminals and are seen as the most likely originators (Chart 4). However activists, foreign governments (or their agencies), third party organisations and employees are all seen as significant.

Employees are seen to be the originators in 31% of cases. Employees have (and continue to be) a significant threat to companies, with their internal defences more at risk. In a recent study by the European Centre for Media, Data and Society[1], over half (56%) of European data breaches from 2005-2014 involved problems internal to the organisation e.g. insider abuse or theft, hardware issues and administrative errors. Criminal hackers accounted for 42% of cases.

The human factor or human error is a common thread we see in most attacks e.g. an employee opening a phishing email, accessing risky websites, losing a laptop or demonstrating lax protection of passwords. Or exhibiting a less than robust reaction to an incident. The education of employees as a first line of defence or, at least, to be aware that they can open the door to an attack, is critical.

1. Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014 – Center for Media, Data and Society, 2014: http://cmds.ceu.edu/article/2014-10-07/data-breaches-europe-reported-breaches-compromised-personal-records-europe-2005.

Implications for companies

Cyber security risk management and associated insurance arrangements need to take centre stage at board level. Of the companies surveyed, 44% had cyber insurance in place, with a further 8% having considered cyber cover. A significant minority, 18%, had not considered having cyber insurance cover and as many as 31% were not aware if their company had cyber insurance in place. They should be. Gaps in coverage, from existing insurance policies not being joined up, mean increased exposure to cyber risk and more. To help companies understand about how they should respond to the increased cyber threat, AIG have written a paper ('Achieving Cyber Resilience'), which has been published by the Geneva Association.

AIG believes there are 5 key questions companies should be asking themselves as the cyber threat continues to evolve.

1. Does your company have regular reporting to and representation among the Group's board of Directors, to ensure a clear understanding of current risk profile and strategy?
2. Does your company monitor the cyber risk landscape effectively as risks evolve?
3. Are you involving third party experts enough (as opposed to in house), to ensure adequate risk mitigation?
4. Do you have the specific Cyber coverage for your needs in the event of a claim?
5. Have you reviewed your insurance policies (including D&O) to understand how they might respond to a possible Cyber incident?

To understand more about how companies should respond to the increased cyber threat, please see our detailed briefing Achieving Cyber Resilience, published by The Geneva Association.

About the author

Mark Camillo is Head of Cyber and Professional Indemnity, EMEA at AIG Europe Limited.

Technical note:

Ipsos MORI conducted 108 interviews with respondents from top 500 companies by turnover and top 100 by capital employed in the UK. Respondents were Chairman, Chief Executive Officers, Managing Directors/ Chief Operating Officers, Financial Directors or other executive board directors. Interviews were carried out face to face (4 were carried out over the telephone) between September and December 2014.

www.aig.com

BELFAST
Forsyth House
Cromac Square
Belfast BT2 8LA
Tel: 02890 726002
Fax: 02890 726085

BIRMINGHAM
Embassy House
60 Church Street
Birmingham B3 2DJ
Tel: 0121 236 9471
Fax: 0121 233 3597

CROYDON
2-8 Altyre Road
Croydon, Surrey CR9 2LG
Tel: 020 8681 2556
Fax: 020 8680 7158

GLASGOW
Centenary House
69 Wellington Street
Glasgow G2 6HJ
Tel: 0141 303 4400
Fax: 0141 303 4440

LEEDS
5th Floor Gallery House
123-131 The Headrow
Leeds LS1 5RD
Tel: 0113 242 1177
Fax: 0113 242 1746

LONDON
58 Fenchurch Street
London EC3M 4AB
Tel: 020 7954 7000
Fax: 020 7954 7001

MANCHESTER
4th Floor, 201 Deansgate
Manchester M3 3NW
Tel: 0161 832 8521
Fax: 0161 832 0149

AIG Bring on tomorrow

American International Group, Inc. (AIG) is a leading global insurance organization serving customers in more than 100 countries and jurisdictions. AIG companies serve commercial, institutional, and individual customers through one of the most extensive worldwide property-casualty networks of any insurer. In addition, AIG companies are leading providers of life insurance and retirement services in the United States. AIG common stock is listed on the New York Stock Exchange and the Tokyo Stock Exchange.

Additional information about AIG can be found at www.aig.com | YouTube: www.youtube.com/aig | Twitter: @AIGemea | LinkedIn: www.linkedin.com/company/aig

In Europe, the principal insurance provider is AIG Europe Limited which is registered in England: company number 1486260. Registered address: The AIG Building, 58 Fenchurch Street, London EC3M 4AB. AIG Europe Limited is authorised by the Prudential Regulation Authority and regulated by the Financial Conduct Authority and Prudential Regulation Authority (FRN number 202628). This information can be checked by visiting the FS Register (www.fsa.gov.uk/register/home.do).