MARSH

JUNE, 2013

2013 CYBER RISK SURVEY

CONTENT:

ORGANISATIONS STILL BEHIND THE CURVE

MARSH'S ANNUAL CYBER CONFERENCE, WHICH THIS YEAR TOOK PLACE ON 22–23 MAY 2013, WAS ATTENDED BY 85 RISK MANAGERS FROM A BROAD CROSS-SECTION OF UK INDUSTRIES.

"Cyber attacks are on the rise and this is a risk that is increasingly coming to the attention of risk managers in all industries."

During the event, an informal survey was undertaken using an audience response voting system to understand the views of the risk managers in attendance on a number of key cyber questions. Where appropriate, these results were compared with those from a similar survey in 2012, painting an interesting picture of changing risk perspectives among risk managers over the last year.

Cyber attacks are on the rise and this is a risk that is increasingly coming to the attention of risk managers in all industries. Although the IT department is still the frontline defence against cyber events, other stakeholders, including the board, are starting to take greater ownership of managing cyber risks. However, the perception of the threat hasn't translated into concerted action – particularly with regards to the limited quantification of risks and uncertain planning around required changes to the collection and processing of personal information as a result of proposed EU data protection law.

Despite the increasing familiarity of cyber risks, risk managers surveyed had serious cyber blind spots. Crucially for those organisations, 22% of those in attendance had made no estimates of the financial impact of a cyber attack. The survey suggests that although risk managers are aware of cyber insurance products, 61% are unsure whether the available cover meets their needs. This is particularly unsettling in the context of changes to EU data protection law, set to come in later this year or early next year – 63% of survey respondents are either not planning to make any changes or need to find out more about this critical piece of legislation.

ORGANISATIONS UNDER ATTACK

A key takeaway from the cyber conference survey is that 54% of organisations represented by risk managers in attendance had been subject to a cyber attack in the last three years (see Figure 1). This is a stark rise on the previous year, where 25% had experienced a cyber attack over the previous three years.

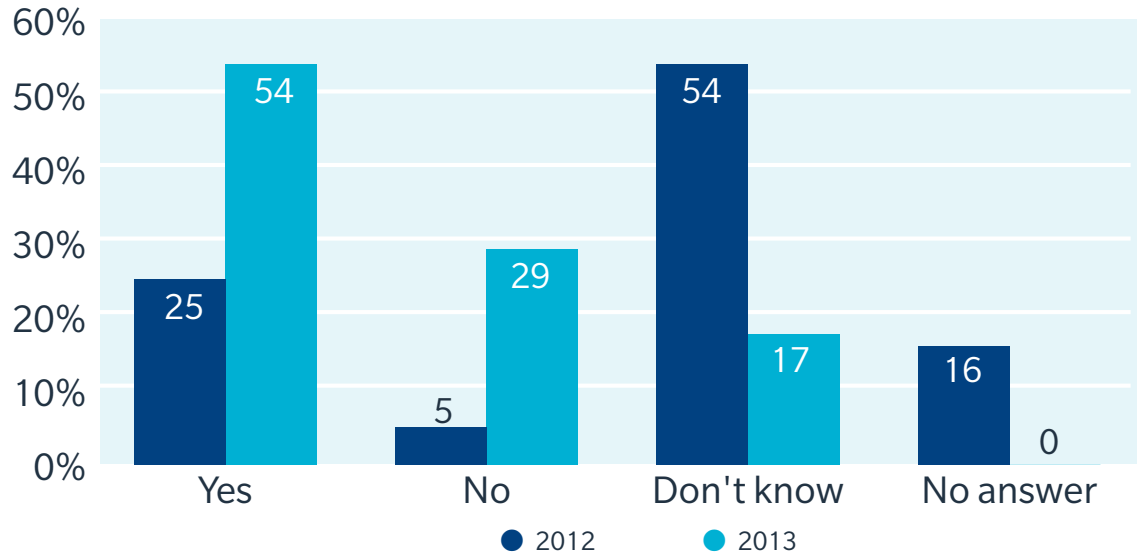
Given the number of attacks these risk managers have faced firsthand, it is no surprise that only 10% of respondents felt that cyber risks are perceived as low risk (see Figure 2). At 53%, the proportion of respondents that qualified cyber risk as either high or very high almost mirrors the number of respondents who have experienced an attack. Even within the context of other items on the risk register, it seems reasonable to assume that the 34% of risk managers that replied "medium" must consider cyber threats to be worthy of serious consideration.

Concern about cyber risk remains high among respondents, with 34% noting concern has risen by a lot and 37% by a little (see Figure 3). This renewed concern is likely driven by a combination of recent and regular cyber breaches and increasing advice from insurers and brokers.

In 2013, just 29% of risk managers think that their mobile phone is safe or very safe from hacking (see Figure 4), while those thinking that their mobile phone is unsafe has risen from 57% to 71% between this survey and the previous. This greater awareness of the vulnerabilities of mobile technology is particularly pertinent in the context of the growing phenomenon of bring your own device (BYOD) technology and the rising number of malware viruses specifically targeting mobile devices.

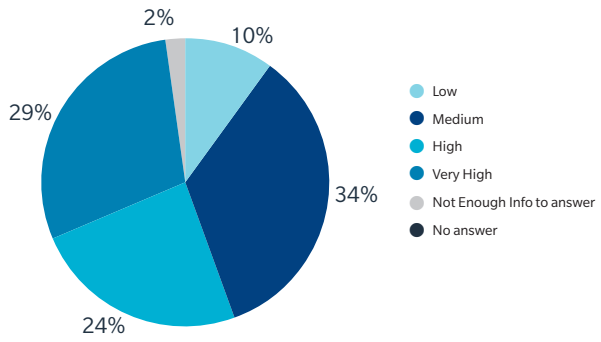
The IT department is still the key hub for managing cyber risk in organisations (see Figure 5), although the trend from 2012 is for the board to take increasing responsibility, having risen from 11% to 20%. This is a clear indication that cyber threats are rising in importance across the organisations surveyed.

FIGURE 1: HAS YOUR ORGANISATION BEEN SUBJECT TO A CYBER ATTACK, SUCCESSFUL OR OTHERWISE, IN THE PAST THREE YEARS?



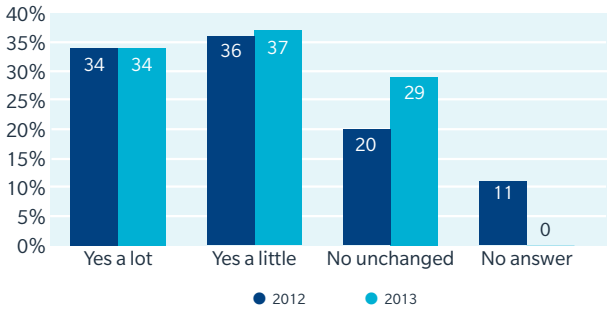
Source: Marsh

FIGURE 2: HOW ARE CYBER RISKS PERCEIVED IN YOUR ORGANISATION (2013)?



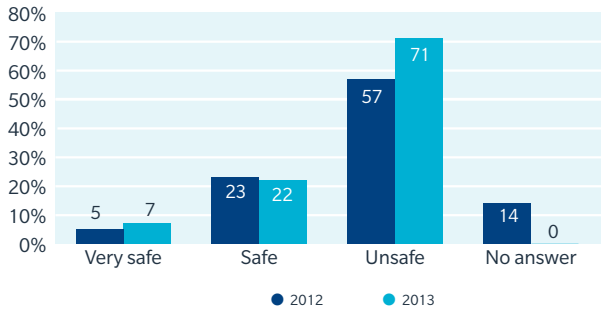
Source: Marsh

FIGURE 3: HAS CONCERN ABOUT CYBER RISK IN YOUR ORGANISATION INCREASED IN THE PAST 12 MONTHS?



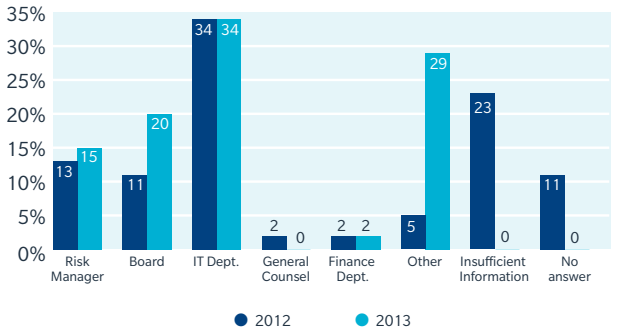
Source: Marsh

FIGURE 4: HOW SAFE FROM HACKING IS YOUR MOBILE PHONE?



Source: Marsh

FIGURE 5: WHO IS RESPONSIBLE FOR MANAGING RISK IN YOUR ORGANISATION?



Source: Marsh

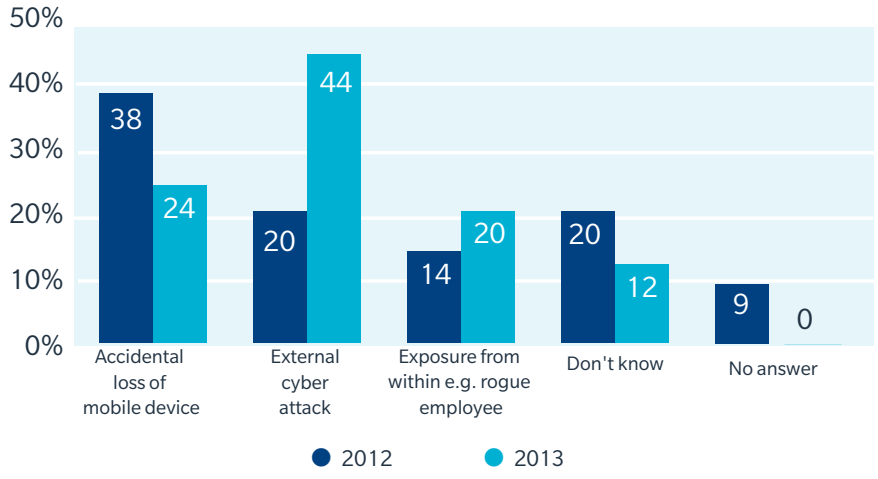
WHAT KEEPS RISKS MANAGERS AWAKE AT NIGHT ?

External cyber attacks came out as the greatest fear at 44% from responding risk managers, followed by accidental loss at 24%, and exposure from within at 20% (See Figure 6). We might have expected the threat from within to feature higher on risk managers' fears, as the threat from a rogue employee, particularly from within the IT department, is usually thought of as significant by all organisations.

The insurance industry seems to be on the right track. To date, it has focused primarily on the loss of customer data and reputational damage and solutions are now widely available for insuring against these top two fears (see Figure 7). The biggest surprise is that business interruption remains as low as 7%, given how dependent upon IT – whether internally or externally managed – organisations are to function. Following high-profile interruptions from cloud failures, and the Business Continuity Institute ranking IT & Telecoms outage at number one in its latest annual survey, the insurance industry has put a lot of work into creating business interruption solutions; organisations' awareness may grow in due course.

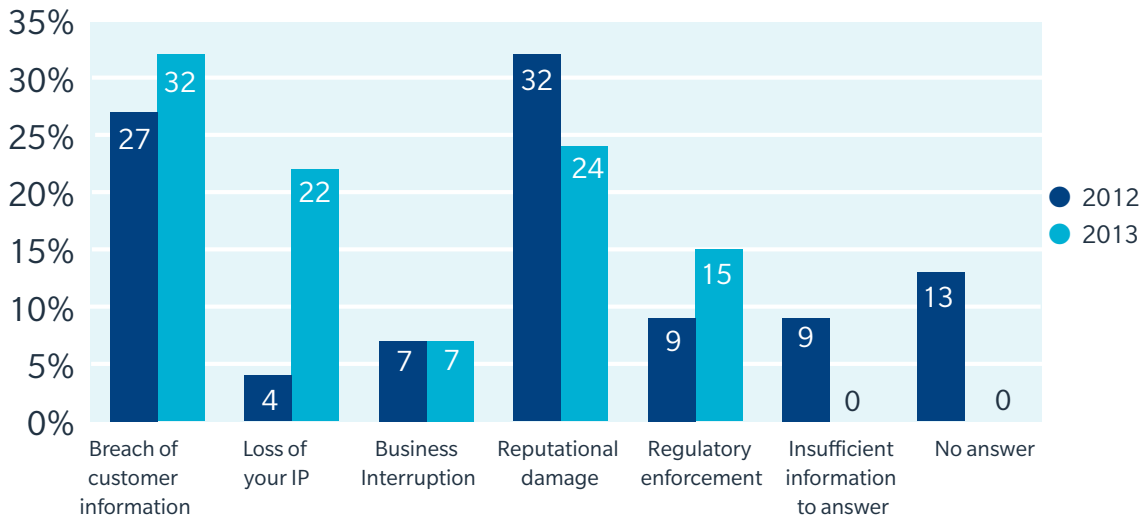
> "External cyber attacks came out as the greatest fear at 44%."

FIGURE 6: WHICH SOURCE OF DATA LOSS IS YOUR ORGANISATION'S GREATEST FEAR?



Source: Marsh

FIGURE 7 : WHICH CYBER LOSS SCENARIO PRESENTS THE GREATEST CONCERN FOR YOUR ORGANISATION ?



Source: Marsh

CYBER ATTACK BLIND SPOTS

Of the organisations that have conducted or estimated the financial impact of a cyber attack, 22% put the figure at $2 million or above (see figure 8). The same percentage of risks managers have made no financial impact estimate and could be exposed to significant risks that have yet to be quantified. Organisations that haven't already done so need to identify and quantify cyber risks so that they can be added to the corporate risk register to ensure the right level of attention and corporate resources are applied to their management.

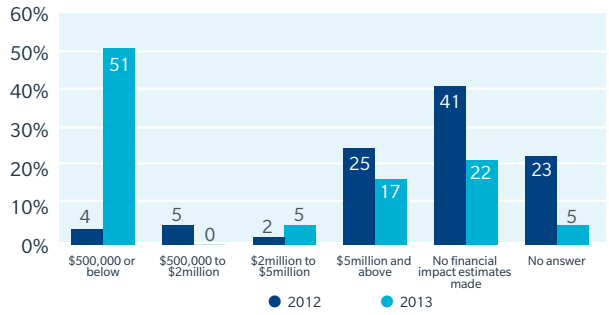
Although most organisations are familiar with cyber insurance – up from 61% last year to 76% this year (see Figure 9) – most risk managers appear to be in the dark about whether the available cover meets their organisation's needs. Because many organisations haven't gone through the process of investigating potential cover in detail, 61% remain unclear about what is available (Figure 10).

Perhaps the most concerning blind spot of risk managers to come out of the survey relates to the understanding and preparedness for reform of the EU's data protection regime, which is expected to introduce new requirements affecting organisations, both operationally and technologically, as well as having the potential to add significant cost to their management of personal data.

While larger organisations are expected to be obliged to have a chief privacy officer, all organisations will face certain operational challenges such as a requirement to delete customer data when requested. However, it is the potentially costly new obligation to notify data subjects when their personal information has been compromised that makes the statistic that just 37% of respondents are aware of planned changes to their insurance and risk management procedures so alarming (see Figure 11).

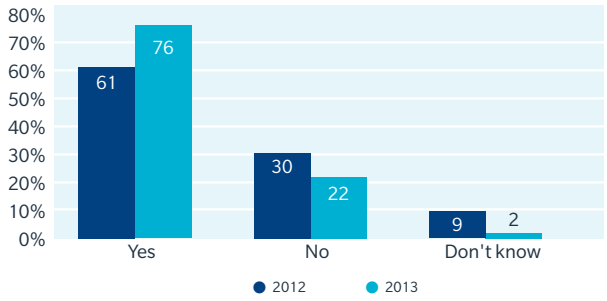
"22% of risks managers that have not made financial impact estimates could be exposed to significant risks."

FIGURE 8: HAS YOUR ORGANISATION CONDUCTED OR ESTIMATED THE FINANCIAL IMPACT OF A CYBER ATTACK? WHAT IS THE FINANCIAL IMPACT?



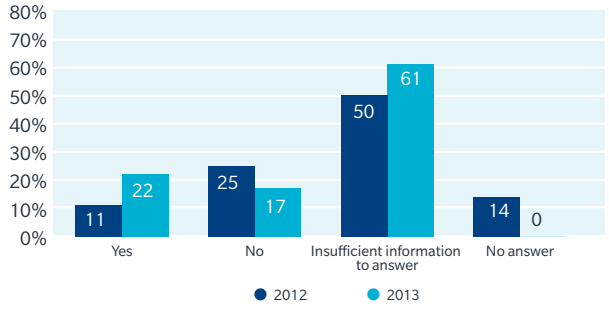
Source: Marsh

FIGURE 9: ARE YOU FAMILIAR WITH CYBER INSURANCE PRODUCTS AVAILABLE IN YOUR MARKETPLACE?



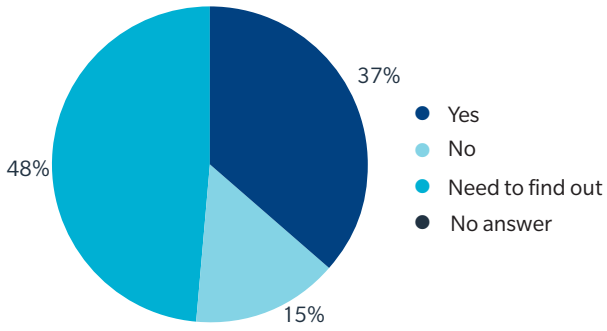
Source: Marsh

FIGURE 10: BASED ON CURRENT KNOWLEDGE DOES AVAILABLE COVER MEET YOUR NEEDS?



Source: Marsh

FIGURE 11: IS YOUR ORGANISATION PLANNING CHANGES TO ITS INSURANCE AND RISK MANAGEMENT PROCEDURES AS A RESULT OF PROPOSED EU DATA PROTECTION LAW (2013)?



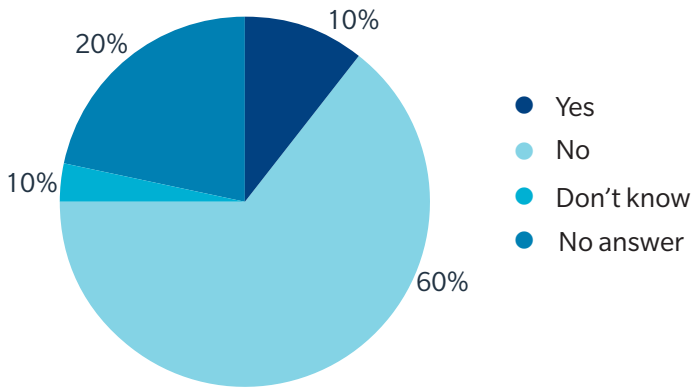
Source: Marsh

CONCLUSION

The insurance industry is clearly targeting areas of cyber risk that are core concerns for organisations. However, it is evident from other results and a low take-up rate at just 10% of those surveyed, that companies have yet to build a detailed understanding of their own unique cyber risk profile in order to make an informed value judgement on the worth of cyber insurance

Greater breadth of stakeholder involvement is encouraging, particularly at board level, with cyber risk no longer being considered the sole preserve of the IT department. As cyber becomes recognised as a business risk rather than a technology problem, we expect to see the shift in ownership result in a deeper understanding of organisations' true financial exposure.

FIGURE 12: DOES YOUR ORGANISATION CURRENTLY BUY CYBER INSURANCE (2013)?



Source: Marsh

MARSH

For further information, please contact your local Marsh office or visit our website at marsh.com

STEPHEN WARES
EMEA Cyber Practice Leader
+44 (0)20 7357 5420
stephen.wares@marsh.com

MARTIN FOLAN
EMEA CMT Industry Analyst
+44 (0)20 7357 3597
martin.folan@marsh.com

 GRAPHICS NO. 13-0483

INSURANCE BROKERS CII CHARTERED