JUNE 2012

CYBER RISK PERCEPTIONS: AN INDUSTRY SNAPSHOT

CONTENT:

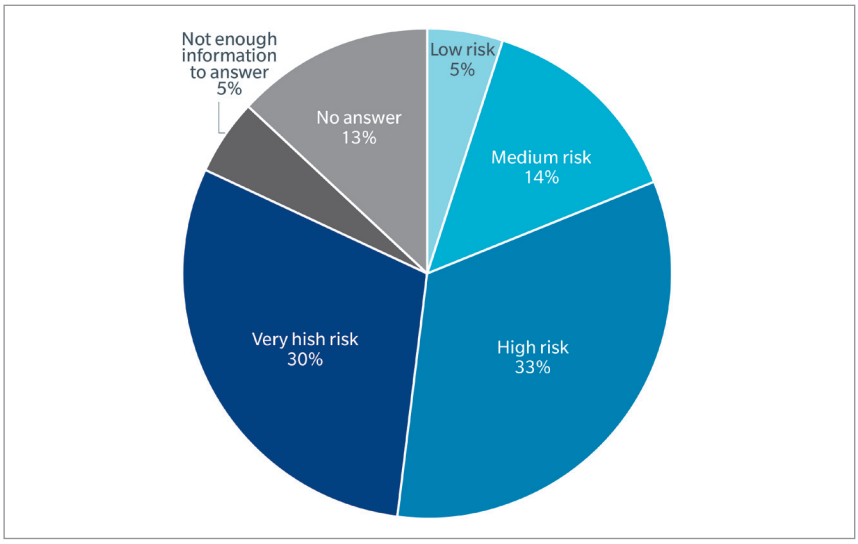
Risk professionals in key industries are looking to the insurers for more innovative risk transfer products in response to a perceived increase in cyber threats to their organisations, according to an informal survey conducted recently by Marsh and Chubb. At the same time, there are indications that the organisations themselves may need to bring more diligence to their treatment and understanding of cyber risks.

CONCERNS OVER CYBER RISK

Cyber risks ranked "high" or "very high" on companies' agendas for over 60 per cent of respondents (see Figure 1) to the Marsh/Chubb survey, which was conducted among 56 attendees at Marsh's annual Communications, Media and Technology (CMT) Conference held in Brighton in early May. Results were further analysed based on respondents' affiliation with two industry groups:

- communication, media, and technology (CMT); and
- financial services, insurance, law and other professional services (FSIP).

FIGURE 1: HOW ARE CYBER RISKS PERCEIVED IN YOUR ORGANISATION?

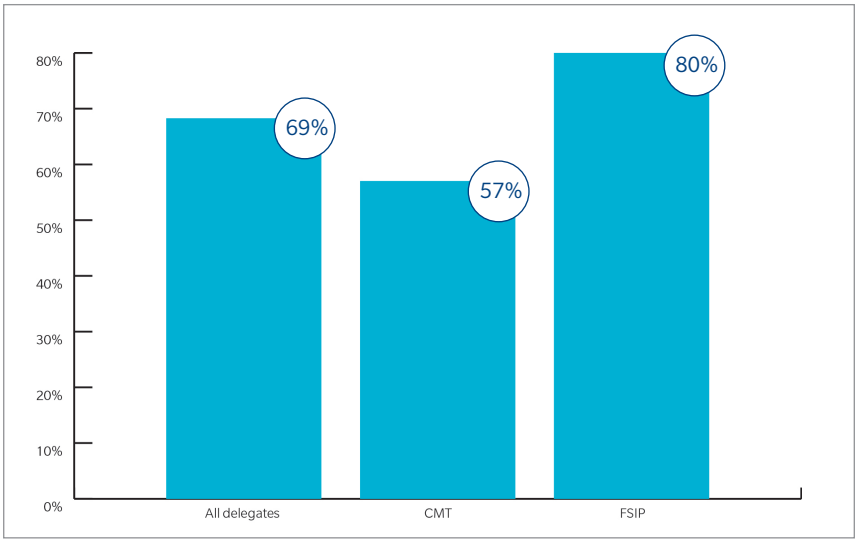


FSIP respondents were more likely than CMT respondents to view cyber risk as high or very high (74 per cent compared to 48 per cent). This difference in perception may be explained by CMT professionals generally being more involved with technology and aware of its attendant risks.

The majority of delegates surveyed said concerns about cyber risk in their organisations have increased over the past 12 months (see Figure 2), including:

- 69 per cent of all delegates surveyed;
- 57 per cent of CMT respondents; and
- 80 per cent of FSIP respondents.

FIGURE 2: HAVE CONCERNS ABOUT CYBER RISK INCREASED IN YOUR ORGANISATION OVER THE PAST 12 MONTHS?



These responses support the general view that cyber risk is a topic of increasing concern in FTSE 250 company boardrooms and elsewhere. This is particularly the case for non-technology companies, which are realising that exposures to technology- and IT-related risks are important and need to be addressed. Because CMT companies typically are on the forefront of cyber developments, it is not entirely surprising that fewer members of that group view cyber risks as having risen over the past 12 months.

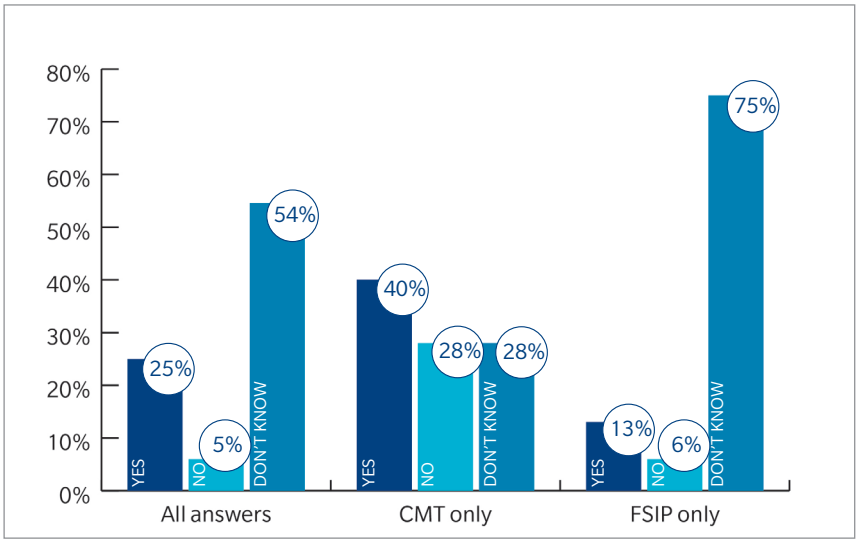
LOW AWARENESS OF CYBER ATTACKS AND POTENTIAL COSTS

One of the more intriguing survey results stemmed from a question about whether organisations had been subject to a cyber attack in the past (see Figure 3). Among respondents overall, 54 per cent said they did not know if there had been an attack at their organisation, 25 per cent said "yes" there had been and 5 per cent said "no" there had not been. It was surprising that only one-third of respondents—people with responsibility for or involved with risk and insurance in their organisations—knew if their organisation ever had been subject to a cyber attack.

- CMT delegates were more likely to have that awareness, with 40 per cent saying their company had been subject to an attack, 28 per cent saying it had not, and 28 per cent saying they did not know.
- Among the FSIP group, however, 75 per cent said they did not know if their company had been the subject of a cyber attack.

This finding suggests that efforts should be made to increase awareness among the insurance and risk management community with respect to cyber risk.

FIGURE 3: HAS YOUR ORGANISATION EVER BEEN SUBJECT TO A CYBER ATTACK?



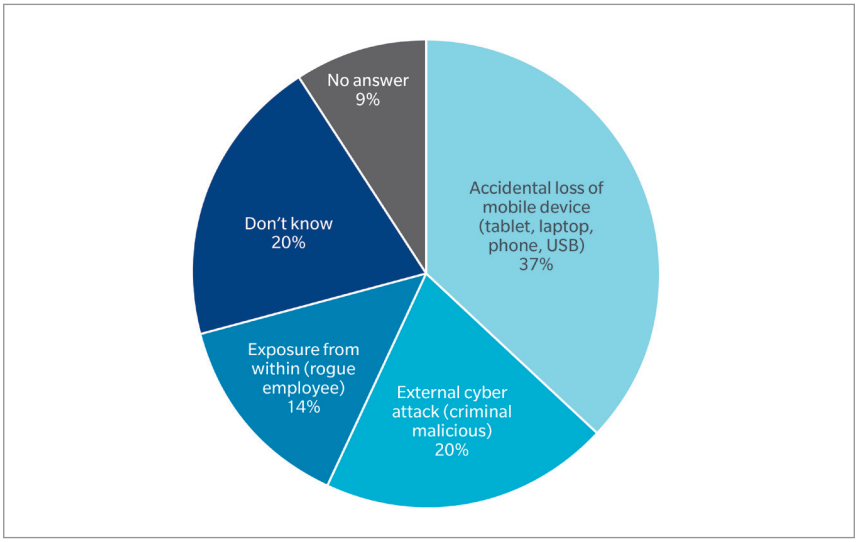
When asked if their organisations had assessed or estimated the financial impact of a cyber attack, 25 per cent of delegates surveyed said that a cyber attack would cost their organisation US$5 million or more. More than half (64 per cent), however, either did not answer or said that no financial impact estimates had been made.

- Among the CMT delegates surveyed:
  - 48 per cent did not answer or answered that no financial impact estimates had been made; and
  - 36 per cent said a cyber attack would cost their organisations US$5 million or more.
- Among the FSIP delegates surveyed:
  - 52 per cent did not answer or answered that no financial impact estimates had been made; and
  - 45 per cent said the financial impact would likely be US$5 million or more.

Regardless of why so few respondents answered the financial damages question affirmatively, more work should be done to adequately assess the financial impact of cyber loss on organisations. The exposures to cyber threats are only likely to increase as dependence on technology and web-based solutions increases. Board members and other stakeholders must be given the information they need to adequately assess the potential financial impact that a cyber event could have on a company.

DATA LOSS FEARS

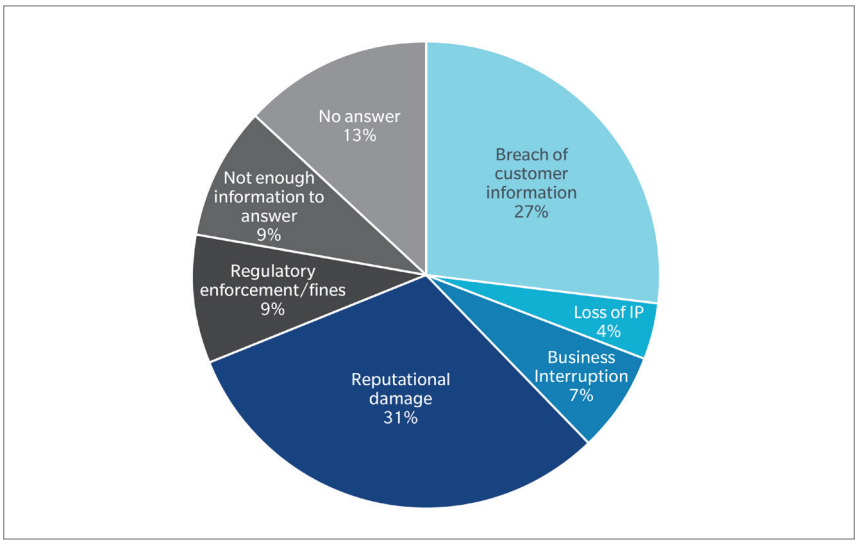
FIGURE 4: WHICH SOURCE OF DATA LOSS IS YOUR ORGANISATION'S GREATEST FEAR?



Data loss is one of the most talked about cyber risks. When asked which source of data loss they feared most (Figure 4), 37 per cent of delegates surveyed said "accidental loss of mobile device" including a tablet, laptop, mobile phone, or USB stick. An external cyber attack was cited by 20 per cent, with 14 per cent citing exposures from within, including from rogue employees.

FIGURE 5: WHICH CYBER LOSS SCENARIO PRESENTS THE GREATEST CONCERN FOR YOUR ORGANISATION?

When asked to choose which out of six cyber loss scenarios represented the one greatest concern for their organisation, 31 per cent of respondents said reputational damage following negative publicity and 27 per cent said breach of customer information. Only 9 per cent of those asked cited concerns about regulatory enforcement, fines, or penalties. These overall percentages aligned with the industry-specific answers.



A significant portion of those surveyed appear to need additional preparation in order to comply with new EU data protection laws that are likely to come into force over the next few years. When asked if their organisations were planning changes to their insurance and risk management procedures as a result of potential changes in the law, 37 per cent said yes, 30 per cent said they needed to find out more, and 13 per cent said no further changes were planned.

- Of the CMT respondents, 28 per cent said they were planning further changes.
- Of the FSIP respondents, 45 per cent said that further changes are planned.

These results may reflect the belief in many companies that there is a large degree of uncertainty regarding the final scope of the laws being considered. Risk managers and others will be well advised to closely monitor this area going forward.

CYBER INSURANCE PRODUCTS

The survey also shone a light on companies' understanding and use of risk transfer measures for cyber risks. Asked whether they were familiar with available cyber insurance products:

- 61 per cent of all delegates surveyed said "yes;"
- 48 per cent of CMT respondents said "yes," with 40 per cent saying "no;" and
- 70 per cent of FSIP delegates said "yes."

It appears that CMT companies would benefit from increased awareness of the insurance solutions available to cover cyber risk.

As to whether their organisations actually purchase cyber insurance:

- 21 per cent of all delegates surveyed said "yes;"
- 28 per cent of CMT respondents said "yes;" and
- 16 per cent of FSIP respondents said "yes."

It is likely that the number of affirmative answers in this group is higher than would be expected if a broader group had been surveyed.

Only 11 per cent of those surveyed said current cyber insurance meets their needs.

- None of the CMT delegates surveyed were satisfied with their current cyber insurance coverage
- Only 19 per cent of the FSIP group felt current cyber coverage meets their needs.

This suggests that current insurance industry offerings are not meeting organisations' overall needs. Coupled with that, those surveyed may have unreasonable expectations regarding what should be available to help them transfer the risk for this emerging and uncertain hazard.

CONCLUSION

As companies come to grips with their increasing cyber exposures, they are likely to turn to the insurance markets for help in mitigating and transferring some of the risks. At the moment, however, insurers either do not have products that are meeting these needs, or have not sufficiently communicated the existence of such products. The results of our informal survey show that there is an opportunity for the insurance markets to innovate and meet the challenges from cyber and related exposure and to meet buyer demands. Concurrently, those involved in risk management within organisations, such as those surveyed here, would do well to increase their own awareness of and dialogue inside their companies about cyber risk.

CONTACT

FREDRIK MOTZFELDT
Europe, Middle East and Africa Leader
Global Communications,
Media & Technology Practice
Marsh

+44 (0)20 7357 5534
fredrik.motzfeldt@marsh.com

MARSH

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

GRAPHICS NO. 12-0632