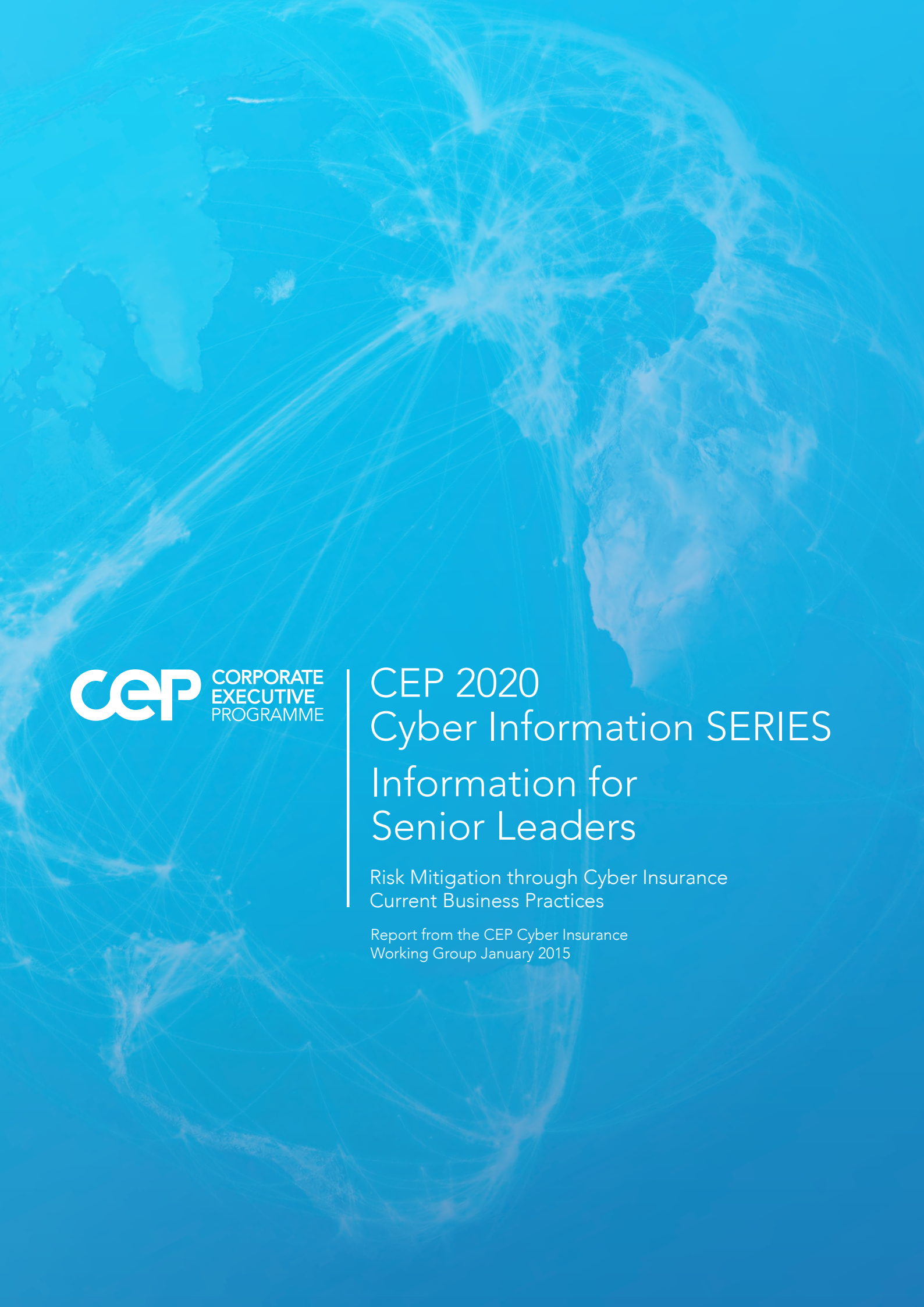


CORPORATE EXECUTIVE PROGRAMME

CEP 2020 Cyber Information SERIES

Information for Senior Leaders

Risk Mitigation through Cyber Insurance Current Business Practices

Report from the CEP Cyber Insurance Working Group January 2015


SECURITY

Welcome

Welcome to the Corporate Executive Programme's 2020 Cyber Information Series. In 2005 twenty seven senior leaders met in Singapore to discuss the many components of information security, and its impact on their organisation's business strategic goals. Ten years on, the CEP is celebrating its tenth anniversary. To mark this important landmark, the CEP is unveiling its 2020 programme. It recognises the technological advances of the last twenty years that have changed the way we work and live e.g. the Internet, Email, Laptops, Smartphones, Wi-Fi to name a few. The 2020 programme recognises that technological change continues and with it, the challenges of applying proactive security. It recognises that the lines between home and office computing are now blurred e.g. many people use only one device for both working at home and at the office. This means there are challenges in the ability to predict threats, identify vulnerabilities and understand associated risks. Our members have all spoken about the benefits gained from the sharing of information, experiences and expertise. The increase in cyber activity and associated malicious activities continues to impact businesses financially globally.

The CEP 2020 Cyber Information Series will feature a series of White Papers on areas that organisations focus on as part of their cyber readiness and cyber management activities. It will highlight the ongoing work of its working groups, sharing with its audiences the outcomes of its research and surveys from which we hope others can benchmark or gather greater understanding for tackling current challenges and issues.

The results of the research carried out by the Working Group on Cyber Insurance are the first in our Cyber Information Series. We hope you enjoy this and the rest of the series.

Foreword

The Corporate Executive Programme (CEP) exists to identify new threats and trends in relation to information security and to help organisations deal with them. Dedicated cyber insurance is one of the newest developments within the marketplace aimed at mitigating risk, and is a product type which has grown somewhat organically out of the growing threat of cybercrime.

It is not an area about which there has been in-depth discussion within industry or between industry and the insurance sector. Although this type of insurance has been available over the last decade, patterns in relation to take-up and business preferences have been unclear and CEP has become aware that a greater understanding would benefit the business and insurance communities.

A CEP working group was set up to explore this subject in 2013, the first time that a not-for-profit organisation had sought to systematically develop understanding in this area for the benefit of business as a whole. It quickly became apparent that research was needed, with the group agreeing on project focus in August 2013 and work starting in autumn that year.

This has been a preliminary study, helping to create a 'snapshot' of current business behaviour and to set the parameters in terms of topics of interest and aspects that would benefit from more in-depth analysis in the future.

It has certainly confirmed that this type of cover is at an early stage in its lifecycle and not particularly well established yet, as illustrated by level of take-up and awareness amongst organisations globally.

The research has also helped to throw some light on the extent to which specific factors are impacting on individual businesses' approach to dedicated cyber insurance; for example, business size, sector and the way companies have organised themselves to manage, and purchase for, risk and security.

CEP will use the findings to help identify the way in which dedicated cyber insurance and risk transfer should be tackled in its future work programme.

We hope that you find this report interesting and informative, and that it helps you with dialogue and making decisions about dedicated cyber insurance within your own organisation.

Dr Claudia Natanson FBCS CITP CISSP
Chair, CEP

chair@globalcep.com

Contents

"Dedicated cyber insurance is one of the newest developments within the marketplace aimed at mitigating risk, and is a product type which has grown somewhat organically out of the growing threat of cybercrime"

Dr Claudia Natanson, Chair CEP

1 Introduction

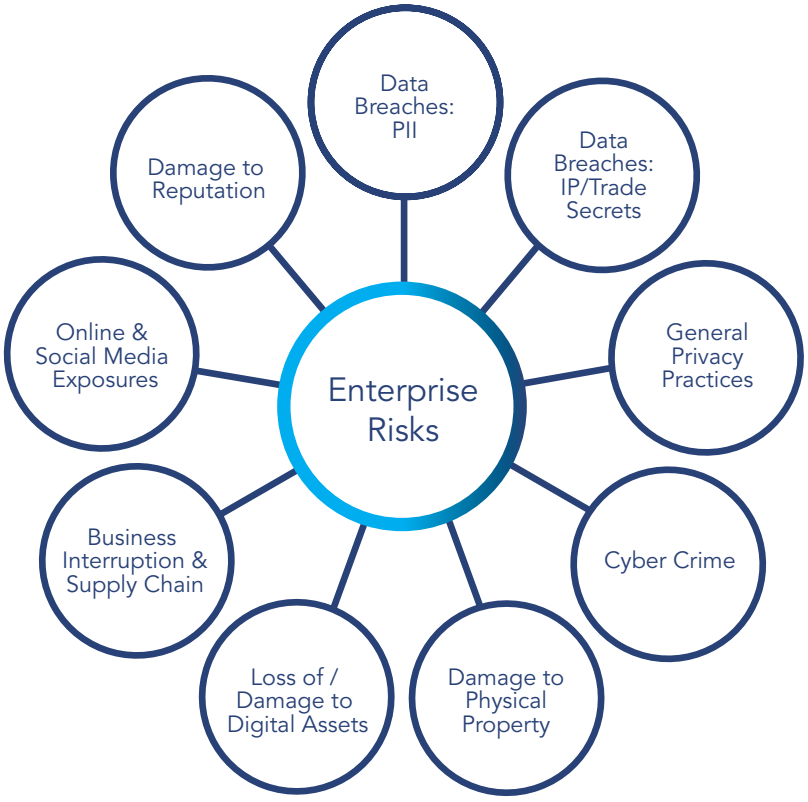
The commercialisation and socialisation of the Internet have brought huge opportunities, but these have been accompanied by significant and continually evolving threats. This has entailed a responsibility for organisations to protect that most valuable asset – their information – and by extension their people, customers and other stakeholders from the damage that could result from it being compromised.

The risks from theft and loss of information are real and growing. Noncompliance with regulations and standards in this area results in damage to brand, revenue, reputation and loss of shareholder and customer confidence. We are seeing more and larger fines relating to failure to protect information adequately, and society's reliance on online technology for the delivery of the most fundamental services is really raising the stakes.

In this climate, organisations are looking to transfer some of the risk for more effective risk management and taking out dedicated cyber insurance is one way they are seeking to achieve this. There are a number of categories of risk against which organisations could potentially seek to insure themselves (Figure 1).

Figure 1: Information security and privacy risks faced by organisations

Enterprise Level Information Security & Privacy Risks



Note: PII – professional indemnity insurance; IP – intellectual property

ZURICH®

Dedicated cyber insurance is a relatively new product, technology is evolving fast and security is always playing catch-up, meaning there is a real challenge involved in objectively identifying companies' needs in relation to insurance and what constitutes an effective dedicated cyber insurance product in specific circumstances.

How much cover is needed, what areas of activity and risk do and should qualify for insurance, who should determine purchase and what does the ideal product look like? These are all questions that need to be answered.

This survey begins to explore these issues for the benefit of both purchaser and insurer. The CEP working group responsible for this research intends that the findings and any follow-up projects the programme carries out will make a significant contribution to bringing clarity to this important new issue for today's organisations, whether they are large or small, global or local.

2 Executive Summary

Only 20% of businesses had dedicated cyber insurance

Heads of information security were not involved in insurance purchase decisions

The US had higher levels of dedicated cyber insurance cover than the UK (40% versus 13%)

- Only 20% of respondents said their organisation had dedicated cyber cover. 20% said they had no cover.
- The legal function was most likely to make cyber cover purchasing decisions (in 50% of cases where such cover existed), followed equally by the head of risk and the Executive/Board-level of the organisation (25%) each. Heads of information security appeared to have little role to play in purchase decisions.
- 25% of respondents said their organisation had suffered a business impacting cyber incident within the last year; 30% of these had dedicated cyber insurance.
- Companies that had experienced an incident and had insurance cover had had this cover before the incident.
- Companies with decentralised risk functions seemed to be more likely to have dedicated cyber insurance than those with centralised functions (31% versus 15%). Companies with centralised risk functions were more likely to be covered by self-insurance or other business policies (28% versus 16%).
- The retail sector had most organisations purchasing cyber cover (37% of those with dedicated cyber insurance in this survey), followed by the finance sector (25%). Self-insurance was mostly done by the manufacturing and finance sectors.
- Every company in the survey had third party and/or outsourcing deals in place. Of the companies with cyber cover, only 50% did thorough checks to confirm continued insurance cover through the supply chain. 70% of those with no cyber cover reported doing checks to see that their third parties had cyber cover.
- The US had considerably higher levels of dedicated cyber cover than the UK (40% versus 13%).
- The most popular route for businesses in the billion pound revenue range was self-insurance (33%) while the most popular for those in the million pound revenue range was cover through existing business policies (31%).
- Most heads of information security interviewed did not have knowledge of the types of dedicated cyber insurance products available.

We now go on to describe methodology, findings and conclusions in more detail.


our personal best
flexible
access
for your own device
8.5 billion
devices
connected by 2012
stronger
integration
for team victory
3,500
How Security Aids Management

3 The Survey Sample

The target population was drawn from within the CEP membership, and consisted of a random sample of 40 organisations. These are organisations that could be said to have good information security awareness in relation to the commercial community as a whole, and typically fall within the larger categories of businesses. We aimed to achieve responses from a good spread of organisations, but as a preliminary, exploratory survey, there were no specific targets in terms of size, global versus local, sector or annual revenue.

The breakdown is detailed in Figure 2 below and Figure 5 on page 11.

Figure 2: Sector breakdown

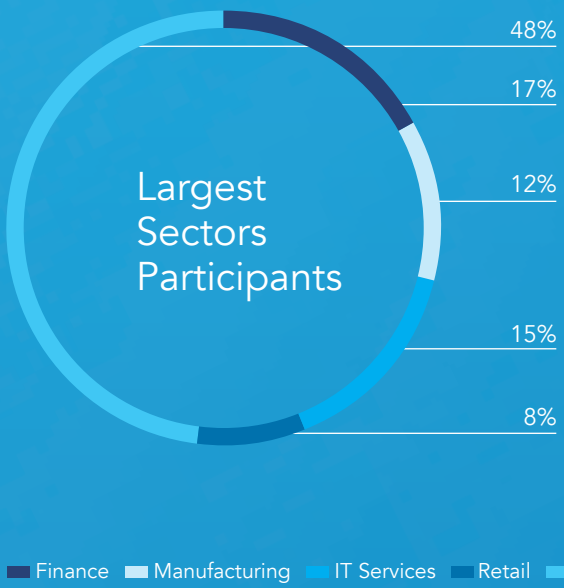


Figure 3: Regional breakdown

The most represented sectors are highlighted in Figure 2. The remaining 48% of respondents came from a wide variety of sectors including; travel, logistics, legal, pharmaceuticals, telecommunications, manufacturing, engineering and marketing.

The size and scope of the sample were selected to successfully reach and carry out interviews with senior leaders on a potentially sensitive subject within reasonable time frames. They also enabled more detailed qualitative discussion. Interviews were undertaken on the basis of maintaining anonymity of respondents and their organisations.

These practical considerations meant that interviews were restricted to US and UK companies. However, this also enabled us to gain an impression of differences between the US and Europe. Traditionally, take up of cyber cover in Europe has lagged behind the USA. The survey aimed to gain insights into whether these regional trends had changed in recent years and, if so, possible drivers for a shift in purchasing patterns.

Figure 4: Revenue breakdown

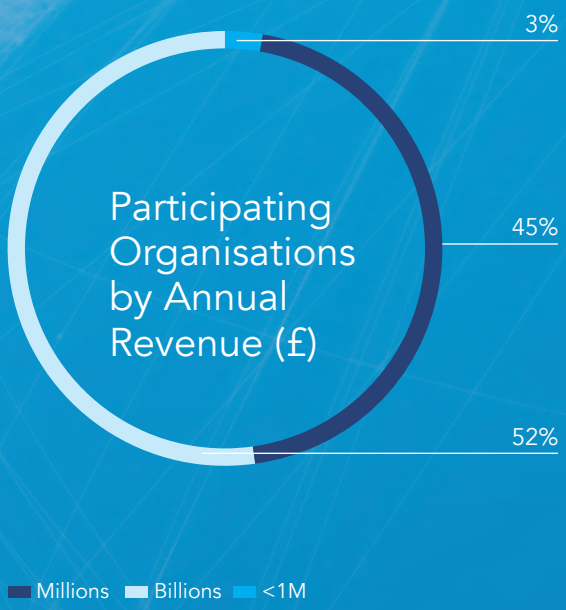
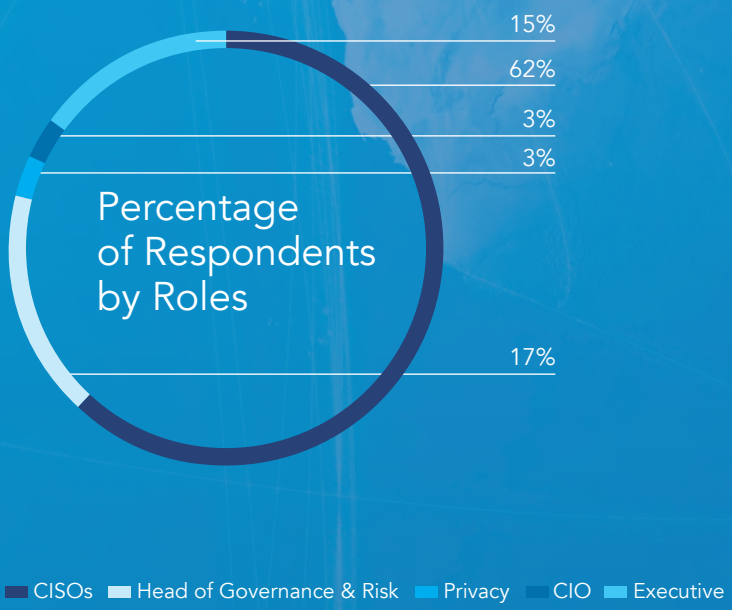


Figure 5: Role of respondents



The survey also considered organisation size to analyse whether any particular purchase trends related to annual turnover. Previous surveys and general industry knowledge had already highlighted the fact that smaller organisations tended not to purchase insurance as the premiums were unaffordable. The current survey was contrasting the behaviours of large and very large global organisations in relation to the transfer of risk through dedicated cyber insurance.

The interviewees were all senior leaders in areas such as risk, privacy, information security and information technology services. The roles were typically chief or head of information security officers (ISO), chief risk officer, chief privacy officer, chief information officer (CIO), head of risk, and head of privacy or insurance services.

4 Survey Methodology

Data was collected by 1:1 telephone or face-to-face interviews

Unless requested, respondents did not receive the questions ahead of the interview as this made it easier to establish accurately levels of current awareness about dedicated cyber insurance and the degree to which they had been involved within their organisation in discussions or decisions relating to purchase of such insurance, or other risk transference activities.

The results were collected and tabulated initially in relation to six key areas:

- Had the company purchased cyber cover?
- What level and scope of dedicated cyber insurance were currently in place?
- Had the company suffered a business impacting cyber incident in the last 12 months?
- Was the risk management function centralised or decentralised within the organisation?
- To what extent was there diligence in managing the supply chain in relation to cyber cover?
- Were best practice standards being employed in information security management, for example; controls, employee training and awareness, security incident event management and security management dashboards?

Using the data gathered, a number of correlations were explored to see if any factors appeared to be encouraging organisations to purchase or defer take up of dedicated cyber insurance cover. The following were considered:

- Was there any apparent relationship between having a centralised or decentralised risk function, and propensity to purchase dedicated cyber insurance?
- Had decisions to purchase been driven by a business impacting incident in the last 12 months?
- Are organisations with cyber cover more likely to display strong best practice standards?
- Are organisations with dedicated roles for leading information security more likely to understand the risks involved and opt to transfer some of these using cyber cover?
- Are larger companies more likely to seek cyber cover?
- Are certain sectors more likely to purchase cyber cover than others?
- Do companies with cyber cover display more or less rigour than those without in checking for cyber cover in their third party supply chain?

5 Definitions

20% said they had cover; 12% did not know

For the purpose of this survey, the following definitions were used:

Dedicated cyber insurance cover: Specific and separate cyber cover, often purchased through an insurance broker who normally gathers information on the level and scope of insurance required from the prospective client.

Self-insurance: This is where organisations set aside their own money to deal with any unexpected potential losses, incidents or contemplated risks.

Coverage by existing policy (business insurance cover): The type of insurance that most organisations take out to cover business disruption that may be caused by any number of factors, ranging from system and network down time, to natural events and disasters such as hurricanes, fires or floods.

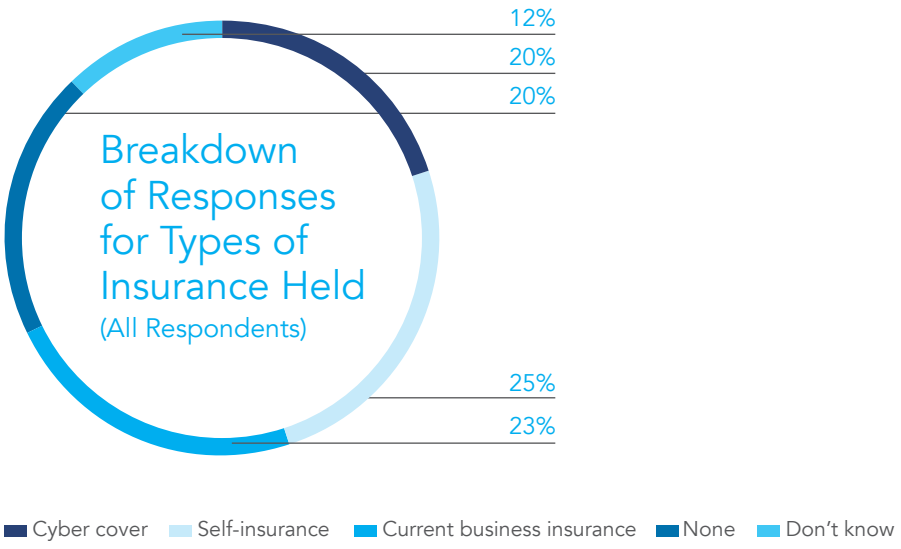
6 Survey Results

Organisations with dedicated cyber insurance

Only 20% of businesses surveyed had dedicated cyber insurance.

25% chose to self-insure, 23% chose to bundle this category of insurance within their existing business policies, 20% said they had no cover and 12% did not know.

Figure 6: Proportions of different insurance types



Respondents said that the following factors had been taken into consideration when selecting the type of insurance cover within their organisation:

1. How to cover the fallout from brand and reputation damage.
2. Protecting income in the event of system failure due to cyber-attacks.
3. The value of the assets being protected.
4. Privacy obligations, the negative business impact of regulatory non-compliance, introduction of data breach notification requirements.
5. Potential impact and risk of cyber extortion activities.
6. Board recommendation.
7. Loss of data and resulting fines arising from third party vendor not being sufficiently insured.
8. How often it was likely to be used, and if so, for what areas.
9. Ensuring sufficient cover in relation to acquisition activities.
10. A respondent who did not take cover said this was as a result of doing a return on investment as well as risk assessment to determine the desirability of taking out dedicated cyber insurance.
11. Another said dedicated cyber insurance was taken out as part of compliance control.

It should also be noted that, in a number of cases, respondents did not know what the major drivers for purchase were.

Survey Results

While the proportion of respondents who did not know if they had relevant insurance or not was relatively low at 12%, levels of uncertainty increased considerably when they were asked if their organisation was covered for specific types of risks (Figure 7). It was evident that, where business cover was being used, some respondents were not entirely sure where or under what sections cyber risks were covered in company insurance.

Insurance Coverage Areas

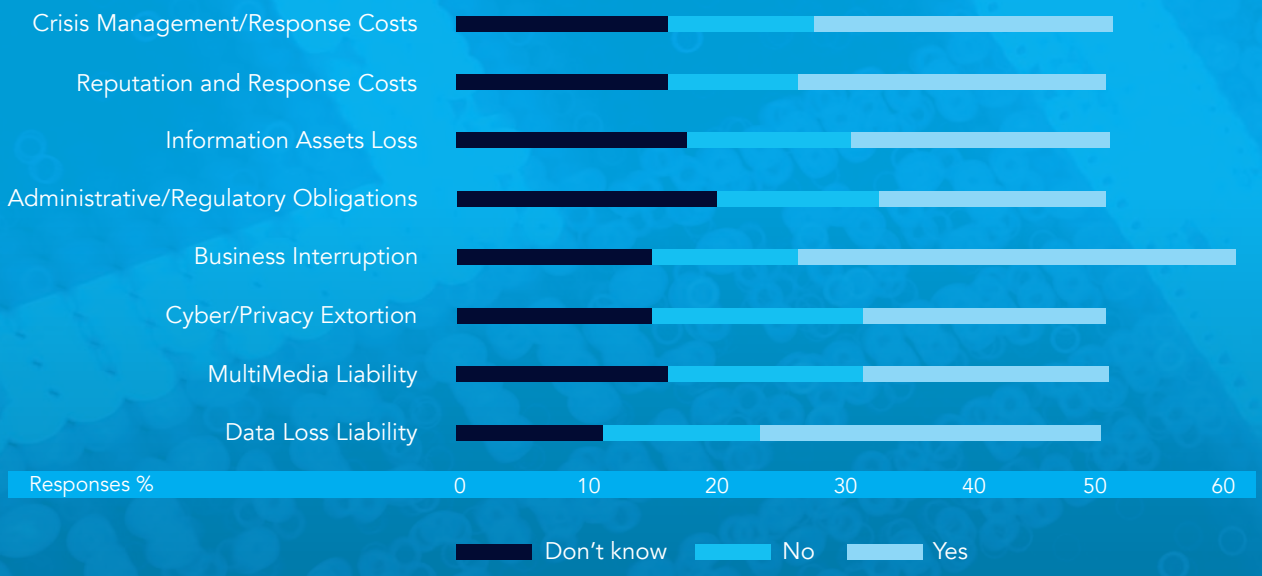


Figure 7: Risks categories for which organisations had insurance cover

Data loss liability	Loss of corporate or personal information through: network security breaches; denial of access to data; destruction of data; disclosure of data
Multimedia liability	Covers third party claims of defamation; infringement of copyright; plagiarism or theft of ideas; invasion of privacy; unfair competition
Cyber/privacy extortion	Responds to threat of intentional security attacks by an outsider attempting to extort money, securities or other valuables Covers payments to investigate, prevent, end or settle the threat
Business interruption	Interruption, degradation in service or failure of the network. Covers resultant loss of income, increased cost of operation and/or cost incurred in mitigating and investigating the loss
Administrative/regulatory obligations	Covers cost of data administration investigations and fines arising from breach of data protection legislation
Information asset loss	Loss, corruption or destruction of: computer systems, key digital assets, customer databases, or any other information assets held electronically
Reputation and response costs	Arising from a data breach being reported (whether factually correct or not), that results in loss of intellectual property, income, customers and/or increased cost of operation
Crisis management/response costs	Covers notifications (to clients or consumers) of data privacy breach, PR and media relations assistance in managing and mitigating a cyber incident

Survey Results

Levels of cyber insurance in Europe may increase with EU data breach notification rules

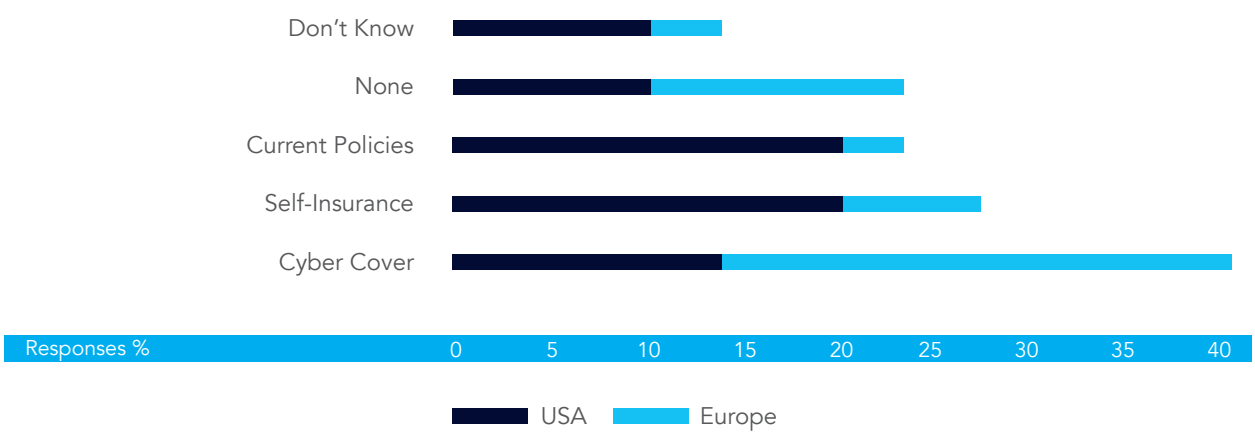
Given the levels of uncertainty, it is also quite possible that some respondents stated that their organisation had no cover when, in fact, this aspect was included in another policy or was self-insured and they either did not know this or were not interpreting this as dedicated cyber insurance.

The survey was not able to tease out the nuances of interpretation of each individual respondent, but, overall, interviews suggested this is an area that is not that familiar to or a priority for a number of those interviewed.

In terms of country analysis, the US was considered separately because of the more punitive measures in existence there relating to information security breaches. For example, 47 US states now have breach notifications in force. The US had much higher levels of dedicated cyber insurance (40% versus 13%). It also had a much smaller proportion of companies without any cyber cover (10% versus 23%).

This apparent trend for lower levels of dedicated cyber insurance in the European region may change with the pending EU data breach notification rules for data controllers under the draft General Data Protection Regulation and the proposed cyber breach notification rules for critical infrastructure providers under the draft Network and Information Security Directive. These changes could become a catalyst for an upsurge in cyber cover in Europe.

Figure 8: Type of insurance cover by region



Dedicated cyber insurance was most commonly in place in the retail sector, followed by the finance sector

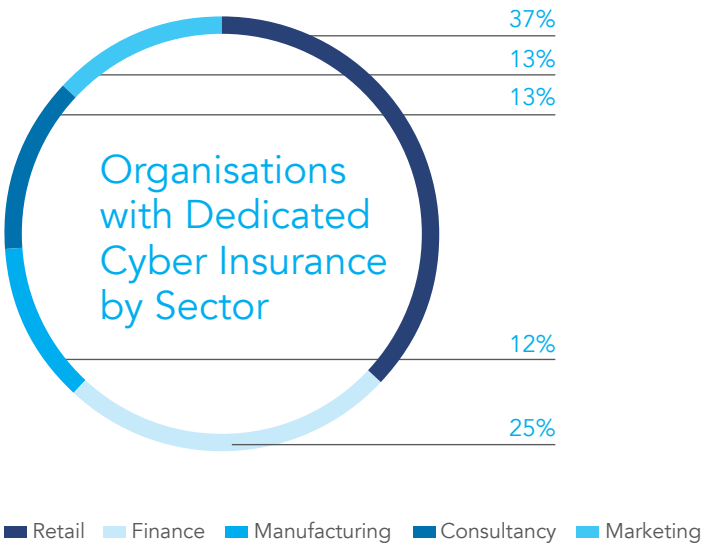
Industry sector

The retail sector made up the highest proportion of companies with dedicated cyber insurance, representing 37% of take-up. This may relate to perceived additional risk arising from: holding of large consumer databases; accumulating a considerable amount of information about purchasers, including confidential financial data; and the importance of online systems functioning 24/7 to achieve sales targets.

The finance sector had the next highest take-up of dedicated cyber insurance (25%). Again, this may relate to their own specific circumstances in holding a considerable amount of personal financial data.

Self-insurance was most common within the manufacturing and finance sectors.

Figure 9: Breakdown of companies with dedicated cyber cover by sector



Survey Results

Organisations with decentralised risk functions were more likely to have dedicated cyber insurance (31% versus 15% for centralised functions)

Management structure and decision-making

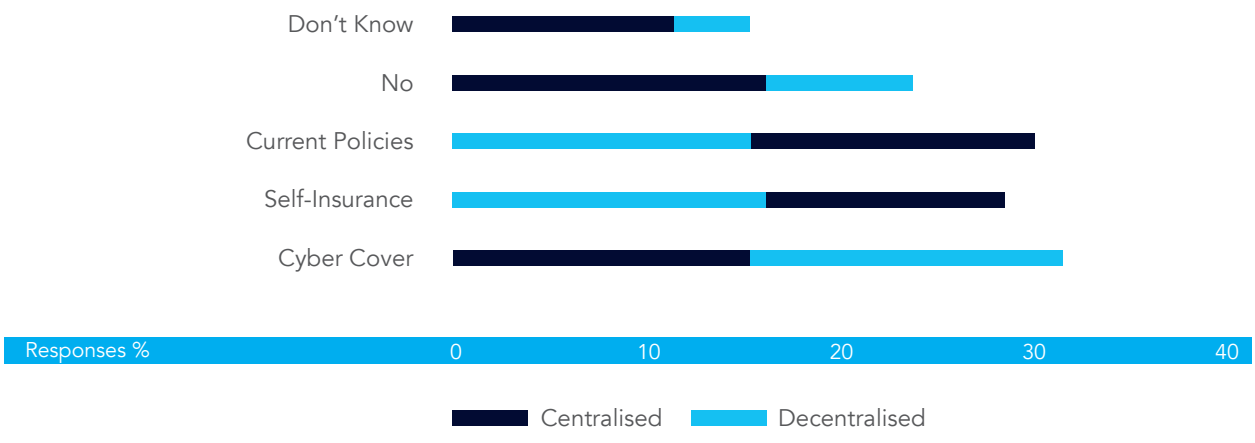
An area of interest for the survey was whether there was any relationship between having a centralised or decentralised risk function, and the likelihood of having dedicated cyber insurance.

68% of organisations had a centralised risk management function, with the remainder being decentralised. By centralised we mean there was one risk function that managed risk across the entire organisation. Various regions and functions would feed information to the centralised risk function. This function would also monitor risk activities across the organisation, then feeding this up to the organisation's audit and risk committee which monitors and manages the organisation's risk at Board level.

A decentralised risk function was deemed to apply to those organisations which handled risk locally within their regions, also making risk management decisions locally.

It was interesting to see that a higher proportion of respondents in organisations with decentralised risk functions had dedicated cyber insurance (31% versus 15%). Self-insurance and use of general business policies was more popular with organisations with centralised functions.

Figure 10: Insurance cover – centralised vs. decentralised risk functions



57% of organisations had a CISO, but they were not insurance decision makers

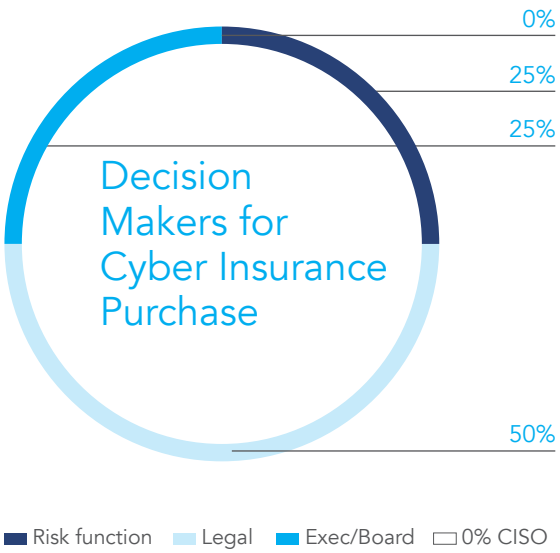
One possible explanation for this is that, where a centralised function exists, the organisation can look at risk to the whole business from an aggregated point of view. With a decentralised function, the picture is more fragmented and may be less easy to pull together, making it difficult to do a comprehensive and objective weighing up of risks. This may mean that such organisations are more inclined to take on dedicated cyber insurance fairly automatically, as a kind of risk catchall.

The survey showed no clear links between the existence of a head of information security and likelihood of taking out dedicated cyber insurance.

57% of organisations had a chief information security officer/head of information security, but only 20% of these had opted for dedicated cyber insurance.

We know that it would typically be the responsibility of the head of information security to deal with information breaches and cyber incidents, along with key stakeholders across the business, when they occur. However, it was apparent over the course of interviews and where dedicated cyber insurance was in place that this role did not seem to be taking a direct role in purchase decisions. **Not one respondent said their CISO was an insurance purchase decision maker**. The legal function made the purchasing decisions in half of cases, followed by the head of risk (25%) or someone at Executive/Board level (25%).

Figure 11: Roles taking purchase decisions for dedicated cyber insurance



In addition, most of the heads of information security interviewed did not have a knowledge or understanding of the types of dedicated cyber insurance products that were available.

Survey Results

There was no obvious link between whether a risk function was centralised or decentralised, and levels of cyber incidents

Cyber incident in previous 12 months

25% of those interviewed said that their organisation had suffered a major business impacting cyber incident within the last year, and 30% of these had dedicated cyber insurance cover. However, the companies with cover had all had this prior to the event, so the incidents played no part in their decision to purchase dedicated cyber insurance.

It was beyond the scope of this survey to examine the relationship between having a centralised or decentralised risk function, and effectiveness in clearing up any incident that may arise.

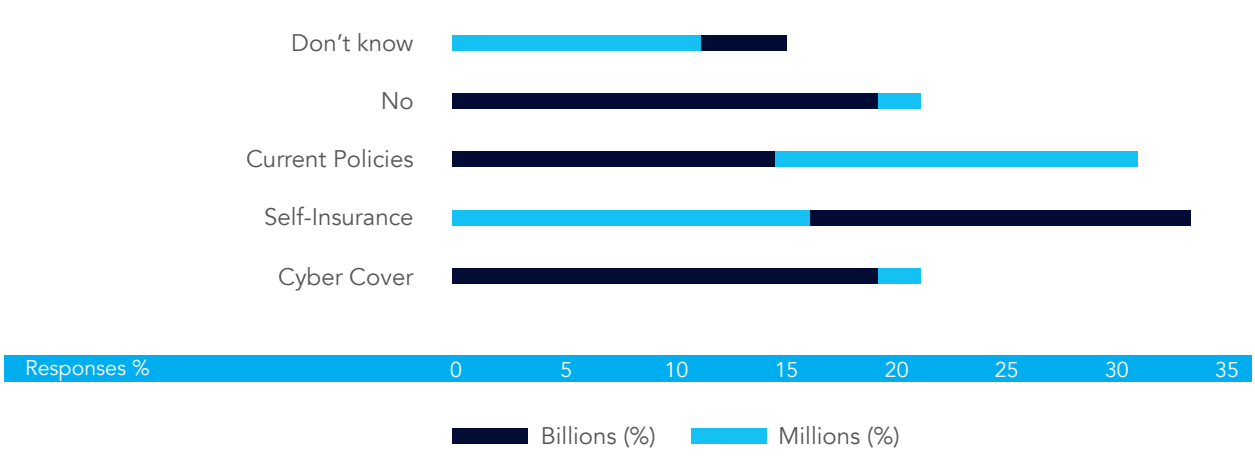
Almost all (95%) of respondents said they had in place information security controls, awareness programmes and training and an effective dashboard to monitor effectiveness. It was beyond the remit of this research to measure and analyse actual performance.

It was, therefore, not possible to establish a link between standards of information security management and whether dedicated cyber insurance was in place or not.

Size of the organisation

The most popular route for businesses in the billion pound revenue range was self-insurance (33%) while the most popular for those in the million pound revenue range was cover through existing business policies (32%). Similar proportions of the two groups had dedicated cyber insurance or no relevant insurance (19% of the £bn companies and 21% of the £m companies in both cases).

Figure 12: Comparison of type of insurance by size of company (revenue)



Cyber cover was most commonly through self-insurance for £bn revenue companies, existing business policies for £m companies

It also emerged in the course of interviews that some of the very large businesses had experienced incidents where the 'mop-up' cost had not been financially devastating, and this had increased their reluctance to go down the cyber cover route.

This survey did not cover many businesses in the SME category, so could not provide a comparison of the proportion of these taking dedicated cyber insurance versus larger organisations. This is an area that will be looked at in future research.

Companies with no dedicated cyber insurance were more likely to check if their suppliers had it than those with cyber cover (70% versus 50%)

The supply chain

Every company in the survey had third party or outsourcing agreements in place.

Of the companies with dedicated cyber insurance, only 50% did thorough checks on third parties to confirm continued insurance cover through the supply chain. Of those with no dedicated cyber insurance, 70% checked to see if their suppliers had cyber cover. This may have been because the insured felt that they were covered by their own policies for anything that happened within the supply chain. It was beyond the scope of the survey to investigate these motivations, but this may be an interesting area to explore in future research.

Concern was also expressed that vital suppliers felt unable to buy insurance because of cost.

There was concern that vital suppliers felt unable to buy insurance because of cost

7 Additional Qualitative Findings

Key points arising from discussions with respondents were:

Liaison with insurer

Some felt that taking out dedicated cyber insurance was like being caught up in a financial game, as it was hard to be 100% sure that you would be covered for any specific incident that occurred and sub-limits applying to specific categories of a claim meant that it was quite likely you would not be able to recoup all that the incident had cost the organisation.

One interviewee felt that brokers were sometimes unable to provide adequate guidance to clients, simply because those from both sides involved in discussions did not have a complete understanding of the needs of the business, and the wrong questions were asked when trying to develop a solution.

One respondent felt there was sometimes too much focus on vulnerabilities rather than actual risk. For example, an organisation could have a particular vulnerability but they would be unlikely to suffer a significant adverse incident because of this. Vulnerabilities have to be considered in tandem with the threat landscape to evaluate actual risk, and knee-jerk reactions need to be avoided.

Another said that they were given a questionnaire by the broker that was more IT than risk-based, showing a lack of understanding of the organisation's need to identify and transfer its risks.

Clearly, ineffective liaison can result in the wrong product being selected or failure to take out dedicated cyber insurance when it is actually needed.

Too much emphasis or not enough?

Distributed denial of service attacks: There were concerns that dedicated cyber insurance did not seem to address denial of service attacks (where hackers place huge bogus demands on online systems causing them to collapse and cease to provide the required service). Even when short-lived, these could have a serious business impact.

Fraud: Some interviewees felt that the current focus on cybercrime meant it was all too easy to forget that a significant proportion of business disruption arising from information compromise is caused by fraudulent behaviour and insider threats (for example, obtaining information or money transfers under false pretences), as opposed to always being driven by cybercrime.

PCI DSS versus general data privacy: In recent times, there has been a great deal of emphasis on credit/debit card security in view of the potential for and actual cybercrime in this area. PCI DSS is a high-profile standard to which organisations gain accreditation in order to show they have suitable levels of security for handling these kinds of transactions. Some respondents in the survey felt that there was now too much focus on this area by organisations and a lot of hype about the risks from some vendors, to the detriment of other privacy issues. They reasoned that it should be treated as part of the overall data privacy strategy and best practice should be followed across the board.

System recovery: There were also concerns about lack of clarity over what was included or defined in cover for this area, which relates both to the issue of technical recovery and the costs arising; for example, from notifying those affected and carrying out necessary publicity.

Deals/investments: One respondent from the financial sector felt that deals and investment related personal data did not appear to be covered under dedicated cyber insurance policies.

Geography

Some respondents felt there should be more of a spotlight on geographic regions from which high levels of cybercrime were originating in terms of a sharing framework to understand risks, and discuss approaches to these threats and risk transference in relation to such crimes.

Other interviewees said that not enough information seemed to be available about which countries, if any, would be exempted under dedicated cyber insurance cover. The concern was that in some regions where precautions tended to be less stringent, for example where encryption was not routinely rolled out, there could be a potential adverse impact for cover.

Some felt that they did not have sufficient information on global fines being levied for data breaches and this was adversely affecting their ability to make informed decisions about insurance.

8 Conclusions and Next Steps

Heads of information security should be more involved in dedicated cyber insurance purchase

This survey was able to look at the behaviours of a number of organisations in relation to dedicated cyber insurance.

Although the sample size of this preliminary survey means it has not been possible to make conclusive quantitative deductions, the findings have given us a clearer picture of how organisations are operating, highlighted challenges, helped confirm industry knowledge and suggested current trends, for example:

1 There is relatively low take-up of dedicated cyber insurance currently, even among very large companies.

2 There is a lack of awareness about dedicated cyber insurance, as witnessed by a number of respondents being vague about how their organisation was covered and having little or no knowledge of dedicated cyber insurance options available. This suggests they would benefit from greater sharing of details within their organisation on product options.

3 There is a worrying trend for heads of information security not to be involved in purchasing decisions, considering they are perhaps best placed to understand the level of risk present that needs to be insured against - a case for organisations to take full advantage of the knowledge of those dealing with the challenge on a day-to-day basis.

4 It has been difficult to establish links between take-up of dedicated cyber insurance and factors such as adhering to best practice standards, having a dedicated head of information security, experience of cybercrime. However, there does appear to be a link between sector and likelihood of take-up.

5 There is some concern about complexity and lack of clarity in policies about what precisely is covered and what it will be possible to claim in the event of an incident and feeling purchasers sometimes do not receive the right guidance or the insurer did not have the right focus i.e. establishing the actual risk involved.

6 Some respondents felt they were lacking the information needed to make good, objective decisions about the type and level of insurance they needed as organisations operating globally e.g. in terms of global data breach fines.

Dedicated cyber insurance is probably never going to be an easy, cut and dry product, simply because technology is a moving target, and organisations and insurers will continue to struggle to keep pace with the volume of incidents that arise from known and unknown vulnerabilities.

One important way to help counteract the difficulties and have a clearer picture of what is actually needed is to involve those actually involved in tackling cyber incidents – that is, information security management – in purchasing decisions.

Purchasers and insurers need to work together to understand and ameliorate the challenges each faces. Insurers need to help purchasers to ensure they have the right policy and understand what they have got, and purchasers need to have systems in place for effectively evaluating risk and ensuring this is part of the insurance decision – and be realistic about what level of protection the financial investment they are prepared to make will get them.

There also needs to be a continued, detailed sharing of information between purchasers and insurers about current global threats, conditions and the resulting impact for insurance, as well as their specific needs and challenges in relation to insurance policies.

The survey has also helped to flag up areas where further work would clearly be useful, for example:

a An in-depth look at reasons for purchasing/and not purchasing cyber cover, and why organisations are selecting particular options.

b Research amongst smaller companies to establish their level of understanding of and attitude towards risk mitigation and transfer. The current survey had very few respondents from smaller organisations. It should be noted that such companies are critical to maintaining the security of the type of companies surveyed in this research, for whom they very frequently act as suppliers. It should also be noted that the companies involved in the current survey have relatively high levels of information security awareness, so it is quite likely that we would see lower awareness levels and take-up within the business community at large.

This survey will be discussed within the CEP working group and its findings are being made public. Feedback and views received will be used to develop a plan for additional work in this area.

CORPORATE EXECUTIVE PROGRAMME

About the CEP

The Corporate Executive Programme is a world-wide organisation that promotes collaboration and shared knowledge against security threats and risk. Formed in June 2005 in Singapore, the CEP unites senior decision-makers from the world's leading enterprises and public sector organisations.

The CEP format is unique in that it takes a cross-functional view of risk across an entire organisation including Human Resources, Marketing, Sales, Finance and Information Technology. Due to this enterprise-wide approach, the CEP is specifically geared towards senior leaders. It is also one of the CEP's goals to influence governments in their approach to international threats and risk issues.

Protection of corporate reputation is a major focus of our activities, and that means understanding the various risks that can negatively impact on a company's business growth, revenue stream and relationship with stakeholders. The CEP sees facilitating the achievement of overall business goals and strategic plans as central to all its discussions, recognising that this is at the top of the agenda of its senior-level membership.

Feedback from CEP members indicates a preference for small workshop-type meetings where specific issues are addressed. In addition to peer-to-peer dialogue, solutions to individual corporate problems can be worked through, refined and discussed in a closed, secure, and confidential environment and facilitated by world-renowned risk and industry experts. Our tried and tested format has continued to attract global membership from large and small organisations, who often find themselves working together outside of the CEP in global supply chain.

For more information, contact: info@globalcep.com

CEP Annual Sponsors

Article10

QUALYS® CONTINUOUS SECURITY

ZURICH®

FIRST Improving Security Together

CEP Round Table Sponsors

BT

RSA®

Atos

FIRMUS®

CEP CORPORATE EXECUTIVE PROGRAMME

For more information,
contact: info@globalcep.com

www.globalcep.com