ADVISEN
Insurance Intelligence

2014 NETWORK SECURITY & CYBER RISK MANAGEMENT:

THE THIRD ANNUAL SURVEY OF ENTERPRISE-WIDE CYBER RISK MANAGEMENT PRACTICES IN EUROPE

February 2014

Sponsored by:

ZURICH®

2014 NETWORK SECURITY & CYBER RISK MANAGEMENT:

THE THIRD ANNUAL SURVEY OF ENTERPRISE-WIDE CYBER RISK MANAGEMENT PRACTICES IN EUROPE

Executive Summary

Risk managers, senior executives and board members of European organisations have long recognised that cyber threats could pose a potential danger to their business. Until recently, however, they generally have been reluctant to invest too deeply in measures to help manage the risks. Over the past 12 months it appears that more believe the severity of the threats are increasing along with the impact that they can have on their businesses. As a result, network security risks increasingly were identified as a risk management focus and insurance is playing a much larger role in the cyber risk management strategy for more organisations.

For the third consecutive year, Advisen Ltd and Zurich have partnered on a survey designed to gain insight into the current state and ongoing trends in network security and cyber risk management in Europe.

About the Survey and the Respondents

For the third consecutive year, Advisen Ltd and Zurich have partnered on a survey designed to gain insight into the current state and ongoing trends in network security and cyber risk management in Europe. Conducted for two weeks, the survey began on 28 January, 2014 and concluded on 11 February, 2014. The survey was completed at least in part by 45 risk managers, insurance buyers and other risk professionals.

The largest percentage of respondents (51 percent) classified themselves as Members of Risk Management Departments (Not Head), followed by Chief Risk Manager/Head of Risk Management Department (37 percent) and Other Executive Management (12 percent). Respondents with more than 20 years of risk management experience represented the largest group at 42 percent of the total, followed by 22 percent with between 6 – 10 years, 20 percent with 11-20 years and 13 percent with 5 years or less.

The perceptions of cyber risk among the risk management community continued to grow for the third consecutive year.

The distribution of survey respondents based on the location of their head office is 62 percent UK, 18 percent other EU country, 4 percent Europe other than EU, 9 percent North America, 4 percent Africa and 2 percent Australia/New Zealand. The majority of respondents come from multinational enterprises with 27 percent having branches or subsidiaries in more than 20 countries outside the EU, 27 percent in 6 – 20 countries, 18 percent in 2 – 5 countries and 4 percent in 1 country. 24 percent of respondents come from companies that only operate in their country of origin.

Businesses from an array of industries are represented. Segmented by 13 macro segments, Professional Services accounts for the largest industry sector with 29 percent of the total respondents; followed by Industrials and Consumer Discretionary both at 14 percent; Banks, Energy and Nonbank Financial at 7 percent; Government & Nonprofit, Healthcare, Telecommunications and Utilities at 5 percent; and Consumer Staples at 2 percent.

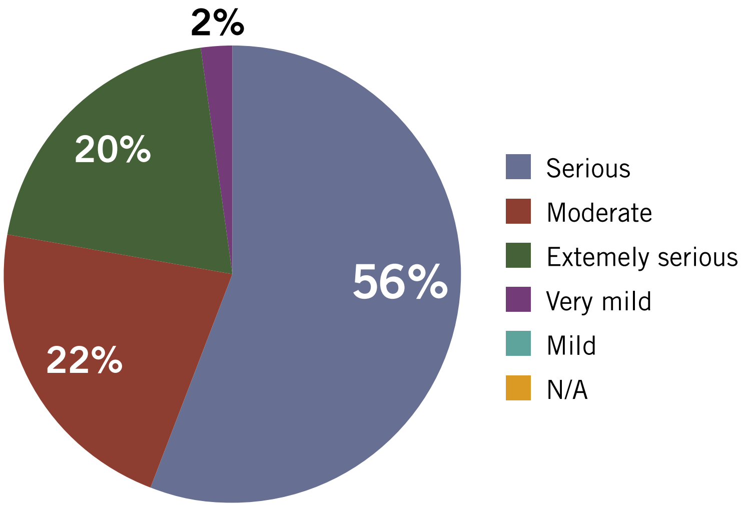
The survey also represents businesses of all sizes but is weighted towards larger companies with 54 percent of respondent companies having annual turnovers in excess of £1 billion. This year respondents also were asked to provide the number of employees. 33 percent have between 5,001 and 15,000 employees, 24 percent have more than 15,000, 22 percent have less than 500, 13 percent between 1,001 and 5,000, and 7 percent between 500 and 1,000 employees.

Perception of Cyber Risk

The perceptions of cyber risk among the risk management community continued to grow for the third consecutive year. The highest percentage of respondents (98 percent) in the three years of this survey said that they believe that cyber risks pose at least a moderate threat to their organisation. This is a 12 percentage point increase from 2013. An even greater jump occurred in the percentage of respondents who believe cyber risks pose a serious or extremely serious threat to their organisation. This group saw a 19 point increase over the previous year from 57 percent in 2013 to 76 percent this year. (Exhibit 1)

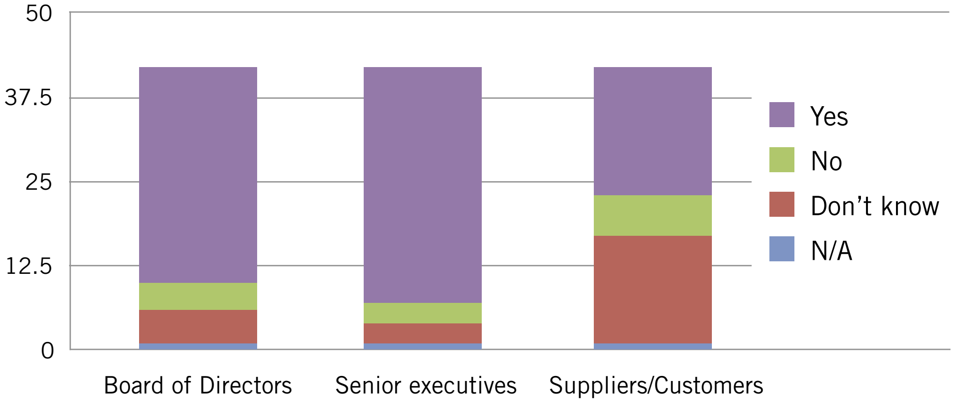
Cyber risks also are increasingly viewed as a threat by both Senior Executives and the Board of Directors.

Exhibit 1: How would you rate the potential dangers posed to your organisation by cyber risks?



Cyber risks also are increasingly viewed as a threat by both Senior Executives and the Board of Directors. In response to the question, "In your experience, are cyber risks viewed as a significant threat to your organisation by:" 76 percent responded "yes" for Board of Directors (53 percent in 2013) and 83 percent responded "yes" for Senior Executives (71 percent in 2013). Additionally, in the three year history of this survey, the highest percentage of respondents (45 percent) said that Suppliers/Customers view cyber risks as a significant threat. This was up 21 points from a year ago. (Exhibit 2)

Exhibit 2: In your experience, are cyber risks viewed as a significant threat to your organisation by:



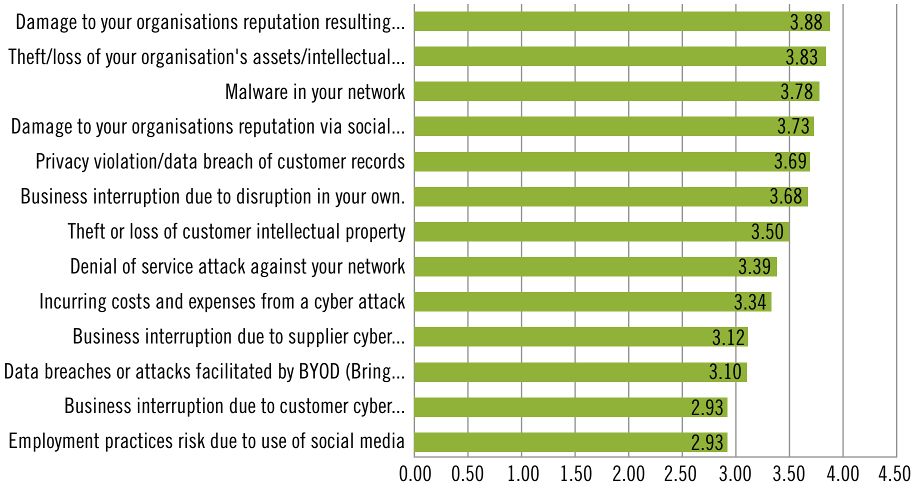
Small and mid-size enterprises (SMEs) can no longer assume that they will be overlooked by cybercriminals. Statistics have shown that they increasingly are targeted because they often have less sophisticated security and can act as a conduit to their larger brethren in today's interconnected world.

Small and mid-size enterprises (SMEs) can no longer assume that they will be overlooked by cybercriminals. Statistics have shown that they increasingly are targeted because they often have less sophisticated security and can act as a conduit to their larger brethren in today's interconnected world. In fact, the smallest companies in this survey (annual turnovers of less than £250 million) viewed cyber threats more seriously than their larger counterparts (annual turnovers greater than £1 billion). 82 percent of the smallest companies believe cyber risk pose a serious or extremely serious threat compared to 76 percent of the larger companies. Cyber threats also are more likely to be viewed as a significant threat at the Board level (92 percent smaller compared to 67 percent larger) and senior executive level (92 percent smaller compared to 71 percent larger).

Respondents were asked to rank specified risks on a scale of 1 to 5, with 5 as very high risk and 1 as very low risk. Based on the weighted average for responses, the biggest concern of this year's respondents is damage to their organisations reputation resulting from a data breach (3.88), followed by theft/loss of their organisations assets/intellectual property (3.83). In contrast, the exposures perceived as representing the lowest risks are employment practice risk due to use of social media and business interruption due to customer cyber disruptions both with a 2.93 weighted average. (Exhibit 3)

For context, last year's biggest concern was denial of service attack or virus on their company's servers (3.55) and lowest was infringing others' intellectual property (2.71).

Exhibit 3: From the perspective of your organisation, please rank the following on a scale of 1 to 5, with 5 as a very high risk and 1 as a very low risk



Sponsored by:

Even businesses or governments with the most sophisticated network security practices and infrastructure are vulnerable to data breaches.

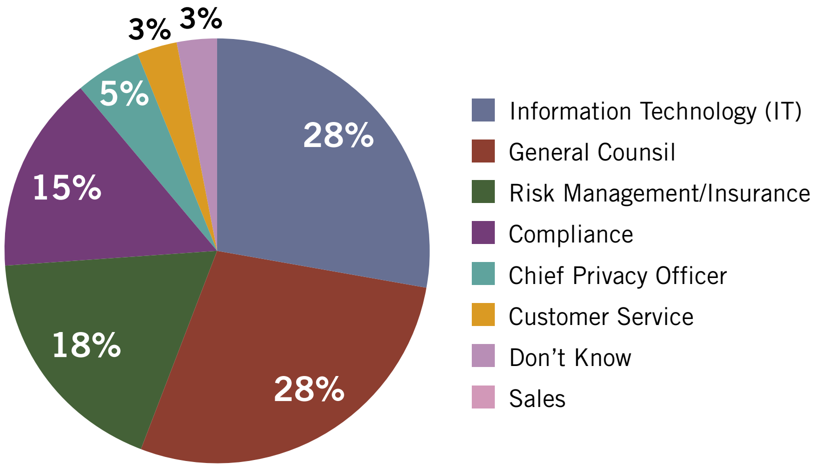
Data Breach Response

Even businesses or governments with the most sophisticated network security practices and infrastructure are vulnerable to data breaches. For this reason it is recommended that they be treated as a "when," rather than an "if," proposition. When a breach does occur, research suggests that organisations who have implemented data breach response plans prior to the breach fare much better than those who have not.

It was with this in mind that respondents were asked, "Does your organisation have a data breach response plan in place in the event of a data breach?" Consistent with last year (59 percent) 55 percent responded "yes." As in previous years, this percentage remains significantly lower than their North American counterparts who were asked the same question in a similar annual survey. In the most recent North American survey from last October, 72 percent responded "yes," – a 17 point difference. Although just over fifty percent of respondents claim to have a data breach response plan in place, the vast majority (83 percent) say that their business continuity planning includes network interruption.

In response to the question "In the event of a data breach, which department in your organisation is most responsible for assuring compliance with applicable privacy laws?" consistent with last year the majority responded either IT (28 percent) or General Counsel (28 percent). (Exhibit 4) If it was determined that customers should be notified of a breach, according to respondents, the departments most commonly responsible for this task are Public Relations at 27 percent, and Customer Service and Compliance, both at 14 percent.

Exhibit 4: In the event of a data breach, which department in your organisation is most responsible for assuring compliance with applicable privacy laws?



Exactly the same percentage of organisations as last year (50 percent) takes a multi-departmental approach to their network security risk management efforts.

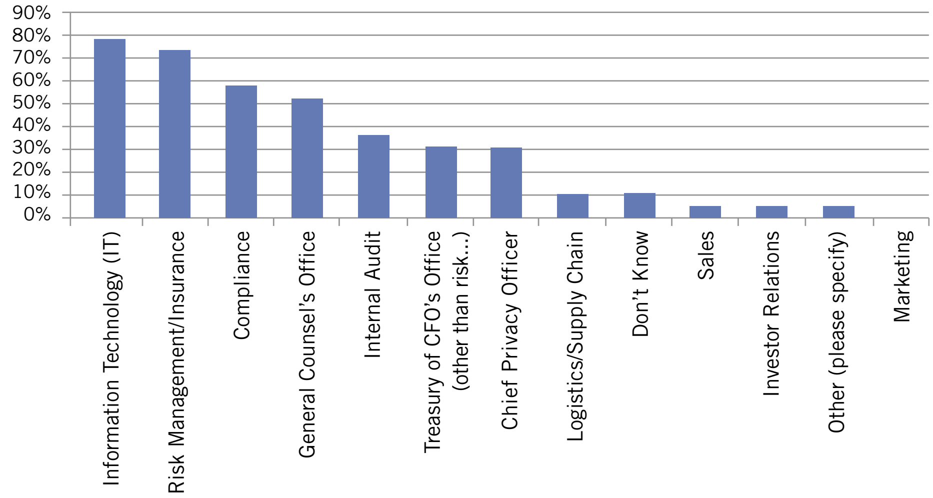
Network Security and Cyber Risk Management Focus

Oranisations increasingly include network security risks as part of their risk management focus. Respondents were asked, “Are network security risks a specific risk management focus with your organisation?” 90 percent responded “yes,” and 10 percent responded “no.” This is the third consecutive year that the percentage of “yes” responses increased up 14 percentage points from 2013 and a total of 20 percentage points since 2012.

Exactly the same percentage of organisations as last year (50 percent) takes a multi-departmental approach to their network security risk management efforts. This varies materially, however, based on the size of company with 62 percent of larger companies (£1 billion or greater) claiming to have this team or committee compared with 33 percent of the smaller companies (under £1 billion). This is consistent with the responses to same question in the North American survey.

The department or functions that are most likely to have representation in the network security risk management team are IT with 79 percent, Risk Management/Insurance 74 percent, Compliance 58 percent, General Counsel 53 percent, Internal Audit 37 percent, Treasury or CFO’s office 32 percent, Chief Privacy Officer 32 percent, Logistics/Supply Chain 11 percent, Investor Relations 5 percent and Sales 5 percent (11 percent Didn’t Know and 5 percent said Other). (Exhibit 5)

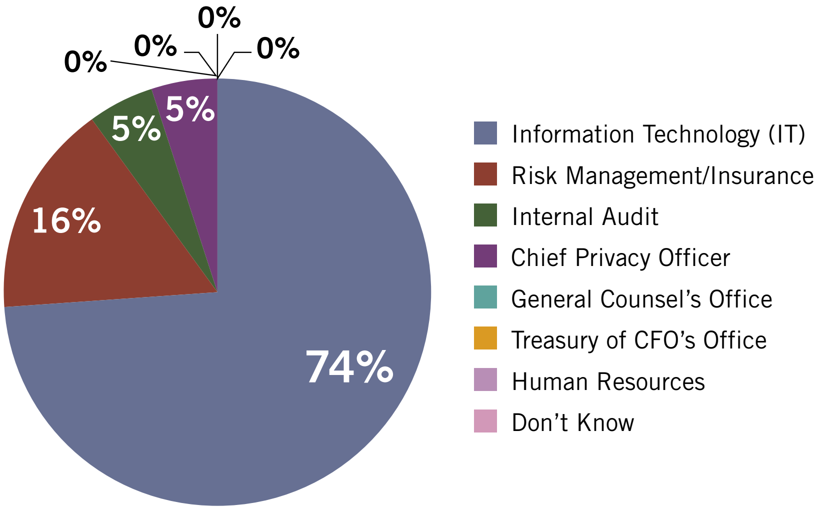
Exhibit 5:
Which departments are represented on this team or committee?



> *By a wide margin, the IT department is still acknowledged as the front line defense against information losses and other cyber risks.*

By a wide margin, the IT department is still acknowledged as the front line defense against information losses and other cyber risks. In response to the question, "Which department is responsible for spearheading the information or network security risk management effort?" 74 percent responded IT with Risk Management/Insurance coming in a distant second with 15 percent. (Exhibit 6)

Exhibit 6: Which department is responsible for spearheading the information or network security risk management effort?



Social Media

Social media can provide businesses with many benefits such as increasing brand awareness, promoting products or providing timely support. It also presents significant risks such as the potential for reputation damage, privacy issues and data breaches. For these reasons, social media is increasingly recognised as an exposure that requires risk management attention. Respondents were asked, "Does your organisation have a written social media policy?" 80 percent responded yes, up a significant 24 percentage points from last year and in-line with the North American survey (76 percent).

Mobile Devices & Cloud Computing

For the second year respondents were asked questions on two increasingly important network security and cyber liability topics, mobile devices and cloud computing. In response to the question, “Does your organisation have a mobile device security policy?” 85 percent responded “yes,” up 16 points from last year.

The popularity and extensive capabilities of smartphones has resulted in many employees preferring to use their personal handheld device for business purposes as opposed to a company issued device. More and more companies are allowing employees to do so, but these non-company controlled devices are accessing proprietary company information and often exposing organisations to a greater degree of risk. When asked, “Does your organisation have a bring-your-own device (BYOD) policy?” 63 percent responded yes, a 22 point increase from 2013.

The popularity and extensive capabilities of smartphones has resulted in many employees preferring to use their personal handheld device for business purposes as opposed to a company issued device.

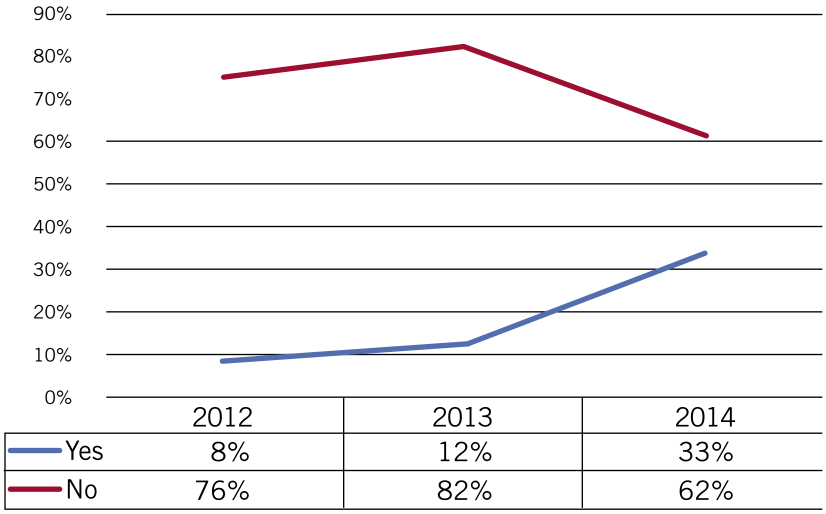
Over the past few years cloud computing has become a popular alternative for businesses seeking to take advantage of its cost effectiveness and increased storage capacity. Warehousing proprietary business information on a third-party server has caused some organisations to question the security of the information being stored. This has become a particular point of concern since it was revealed by U.S. whistleblower Edward Snowden that many of the large cloud service providers such as Google, Apple & Microsoft have been complying with the National Security Agency’s (NSA) request for certain types of data. It appears, however, that the benefits of storing data in the cloud outweigh much of the privacy concerns associated with the technology. When asked, “Does your company use cloud computing services?” 65 percent responded “yes,” a 9 point increase from last year. This shift is also apparent in response to the following question, “Is cloud computing a component of your data security risk management program?” 53 percent responded “yes,” also up 9 percentage points from last year.

The Role of Insurance in Network Security and Cyber Risk Management

The upward trend in the percentage of companies purchasing cyber liability insurance appears to have picked up steam. While still below the levels seen in North America where over half of the respondents claimed to have purchased the cover, the percentage of companies participating in the survey who purchase cyber cover in Europe increased from 12 percent in 2013 to 33 percent this year, a 21 point jump. (Exhibit 7)

> *Companies increasingly recognise the business interruption and reputational consequences a data breach may have on their brand.*

Exhibit 7: Does your organisation purchase cyber liability insurance?



	2012	2013	2014
Yes	8%	12%	33%
No	76%	82%	62%

Of the respondents who purchase coverage, 62 percent said that they have purchased it for less than two years, 31 percent between three and five years, and 8 percent for more than 5 years. 54 percent purchase a stand-alone (monoline) policy and 39 percent purchase it as part of another policy.

Companies increasingly recognise the business interruption and reputational consequences a data breach may have on their brand. With this in mind, respondents who purchase cyber insurance were asked, "Do you currently buy coverage for your loss of income due to data breaches arising from your network?" 46 percent responded "yes" and 54 percent responded "no."

Analysis and Conclusions

After now collecting three consecutive years of data, the network security and cyber risk management picture is becoming much clearer. Trends in attitudes and practices are taking shape and marketplace reactions to emerging issues are presenting themselves. Subsequent surveys will help to provide an even stronger reading into this increasingly important risk management area.

The resounding theme of this year's survey is that more organisations are proactively incorporating cyber strategies into their risk management program and are addressing the full spectrum of cyber risk. Nearly all of the organisations surveyed view cyber risks as at least a moderate threat which was up substantially from previous years and the percentage that view them as severe threats increased dramatically as well. The vast majority of executive and board level management also now views cyber risks as a significant threat.

Cyber threats are no longer only perceived as a large company problem, in fact for the first time a higher percentage of smaller companies believe they pose a serious threat to their organisation and nearly all now make network security a specific risk management focus. But while experts stress that data security is a problem that requires and enterprise-wide solution, only half of the respondents take a multi-departmental approach to managing the risk. This remains a significantly smaller percentage than their North American counterparts.

Cyber threats are no longer only perceived as a large company problem, in fact for the first time a higher percentage of smaller companies believe they pose a serious threat to their organisation and nearly all now make network security a specific risk management focus.

Organisations increasingly are concerned with their exposures from mobile devices and employee use of personal devices and despite the concerns around privacy, cloud computing is gaining in popularity among businesses of all sizes. Although cyber risks are perceived as a moderate threat by nearly all organisations cyber insurance is still not purchased by most but is trending in an upward direction. ■