ADVISEN
Insurance Intelligence®

2015 NETWORK SECURITY & CYBER RISK MANAGEMENT:

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

February 2015

Sponsored by:

ZURICH®

WHITE PAPER

2015 NETWORK SECURITY & CYBER RISK MANAGEMENT:

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

Executive Summary

If risk managers, senior executives and board members of European organisations had any doubt as to the existence of a data security epidemic, the past year likely changed that. With massive data breaches affecting some of the world's biggest companies, nation-states using the cyber realm as a vehicle of war, and businesses sustaining property damage as a result of a cyber-attack, there has been no shortage of cyber related headlines.

For many companies, being involved in a cyber-attack went from a question of "if" to "how bad" will the damage from the inevitable attack be.

Cybercriminal tactics continued to evolve and the ability to execute attacks became easier. For many companies, being involved in a cyber-attack went from a question of "if" to "how bad" will the damage from the inevitable attack be. As a result, network security risks continued to be increasingly recognised as a risk management focus and insurance continues to play a bigger role in the cyber risk management strategy of more organisations.

About the Survey and the Respondents

Advisen Ltd and Zurich have partnered for a fourth year 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 one week, the survey began on 20 January 2015 and concluded on 27 January 2015. Invitations to participate were distributed via email to risk managers, insurance buyers and other risk professionals.

The largest percentage of respondents (42 percent) classified themselves as Members of Risk Management Departments (Not Head), followed by Chief Risk Manager/Head of Risk Management Department (26 percent), Other (26 percent), and Other Executive Management (5 percent). Respondents with more than 20 years of risk management experience represented the largest group at 45 percent of the total, followed by 32 percent with between 11 – 20 years, 18 percent with between 6 – 10 years, and 5 percent with 5 years or less.

The distribution of survey respondents based on the location of their head office is 61 percent UK, 26 percent other EU country, 11 percent Europe other than EU, and 3 percent North America. The majority of respondents come from multinational enterprises with 34 percent having branches or subsidiaries in more than 20 countries outside the EU, 26 percent in 6 – 20 countries, 16 percent in 2-5 countries, and 5 percent in 1 country. Eighteen percent of respondents come from companies that only operate in their country of origin.

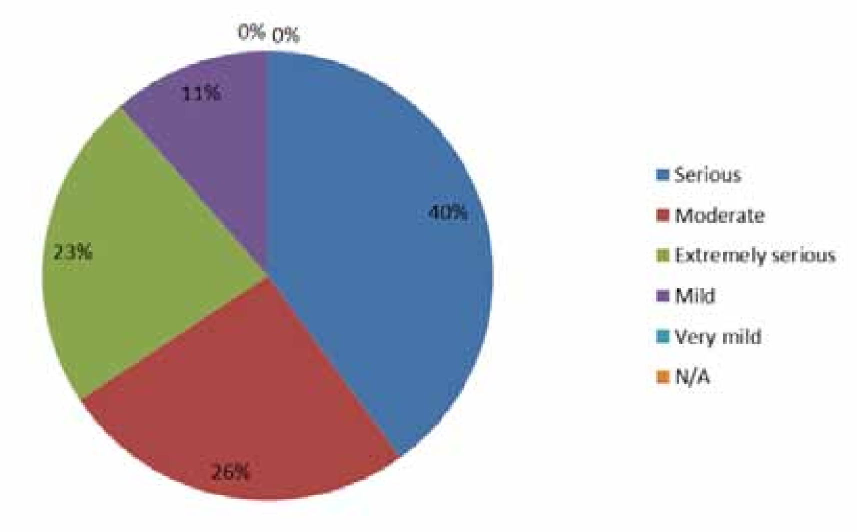
The distribution of survey respondents based on the location of their head office is 61 percent UK, 26 percent other EU country, 11 percent Europe other than EU, and 3 percent North America.

Segmented by 13 macro segments, businesses from an array of industries are represented. The survey also represents businesses of all sizes but is weighted towards larger companies with 76 percent of respondent companies having annual turnovers in excess of £1 billion and 58 percent having excess of 5000 employees.

Perception of Cyber Risk

After three consecutive years of growth, the percentage of the risk management community that perceive cyber risk as at least a moderate threat dropped from 98 percent in 2014 to 89 percent in 2015. This percentage, however, is in-line with the levels seen in the United States where in response to the same question, 88 percent viewed cyber risk as a moderate threat. (Exhibit 1)

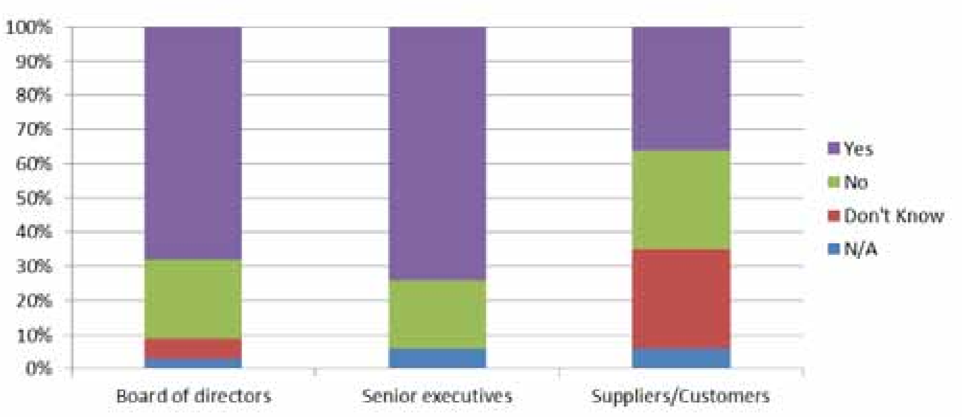
Exhibit 1: How would you rate the potential dangers posed o your organisation by cyber risks?



In contrast, the exposures perceived as representing the lowest risks are "employment practices risk due to use of social media" (2.55) and "business interruption due to customer cyber disruptions" (2.61).

Cyber threats continue to be 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:" 69 percent responded "yes" for Board of Directors, down slightly from 76 percent in 2014 but still above the U.S. at 64 percent. 74 percent responded "yes" for Senior Executives which is also down from 83 percent in 2014 but above the U.S. at 72 percent. Additionally, 37 percent of respondents said that cyber risks are viewed as a significant threat by Suppliers/Customers. This is also down slightly from 45 percent last year but still significantly higher than in 2012 and 2013. (Exhibit 2)

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



Perception of risk varies based on size of business. Although studies have suggested that SMEs are targeted as frequently, if not more so, than larger companies, as a group they continue to view cyber risks less seriously. In response to the question "How would you rate the potential dangers posed to your organisation by cyber risks?" 67 percent of the smallest companies (turnovers less than £1 billion) consider cyber risks to be at least a moderate danger while 96 percent of the largest companies (turnovers greater than £1 billion) consider them to be at least a moderate threat.

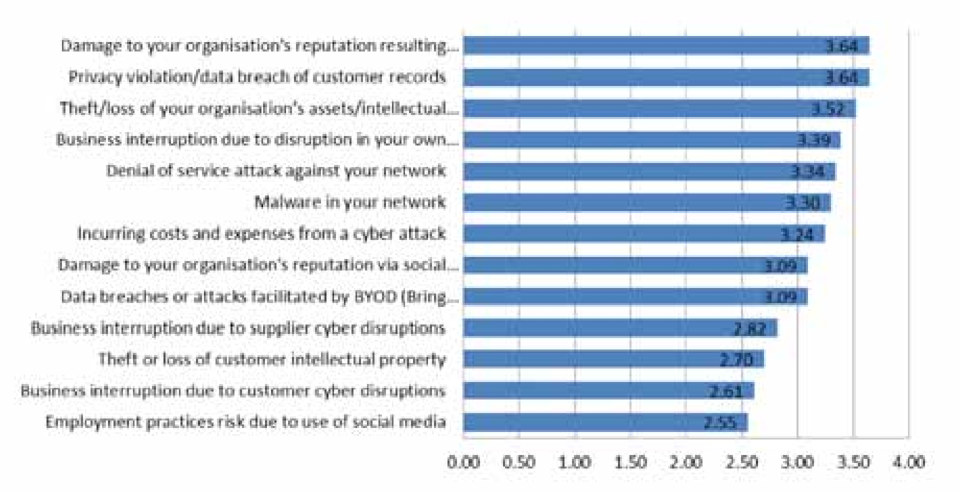
Respondents were asked to rank specified risks on a scale of 1 to 5, with 5 as very high risk and 1 as very low risk. Based on the weighted average, "damage to your organisation's reputation resulting from a data breach" and "privacy violation/data breach of customer records" tied as the biggest concerns of this year's respondents with average of 3.64.

In contrast, the exposures perceived as representing the lowest risks are "employment practices risk due to use of social media" (2.55) and "business interruption due to customer cyber disruptions" (2.61).

When a breach does occur, research suggests that organisations that have data breach response plans in place prior to the incident fare much better than those who do not.

For context, last year's biggest concern was also "damage to your organisation's reputation resulting from a data breach" and the lowest was also "employment practices risk due to use of social media." (Exhibit 3)

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



Data Breach Response

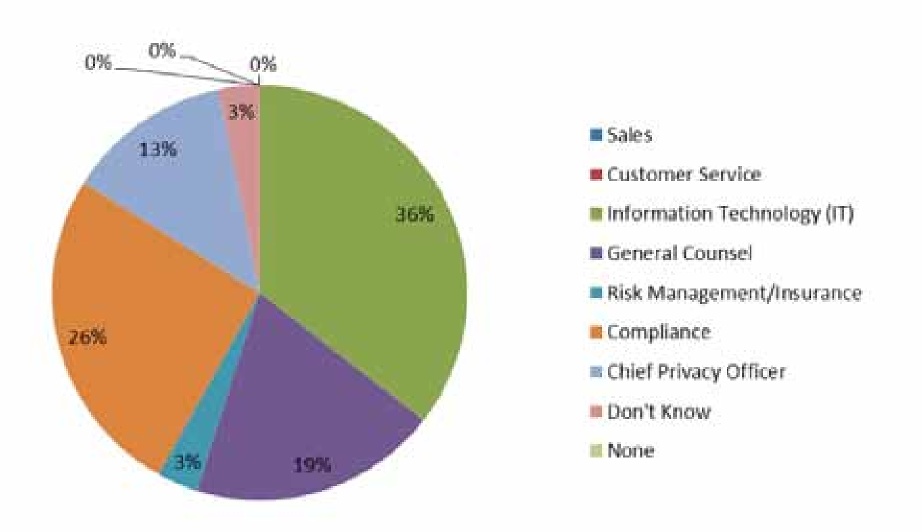
Some of the world's largest and most recognisable businesses have fallen victim to data breaches. These breaches are proof that even the most sophisticated network security practices and infrastructures are vulnerable to a cyber-attack. Some suggest that corporate data breaches are no longer an "if" or even a "when" proposition, but rather "how bad" with the inevitable breach be. When a breach does occur, research suggests that organisations that have data breach response plans in place prior to the incident fare much better than those who do not. It was with this in mind that respondents were asked "Does your organisation have a cyber-incident response plan in place in the event of a data breach?" Consistent with the previous two years, 58 percent responded "yes." As has been the case in previous years, this percentage remains lower than in U.S., but the gap is closing. Last year there was a 17 percentage point difference between the U.S. and European responses to this question. This year the difference is only 4 percentage points.

Although only 58 percent of respondents have implemented a cyber-incident response plan, the vast majority (85 percent) say that their business continuity planning includes network interruption.

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 33 percent and General Counsel at 20 percent.

The majority of respondents (61 percent) believe their organisation is prepared to respond to the data security and privacy laws of all the countries of which they do business. Consistent with previous years, the department most responsible for assuring compliance with the applicable privacy laws is IT according to 36 percent of respondents. Interestingly, however, Compliance (26 percent) edged General Counsel (19 percent) with the second most responses.

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



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 33 percent and General Counsel at 20 percent.

Network Security and Cyber Risk Management Focus

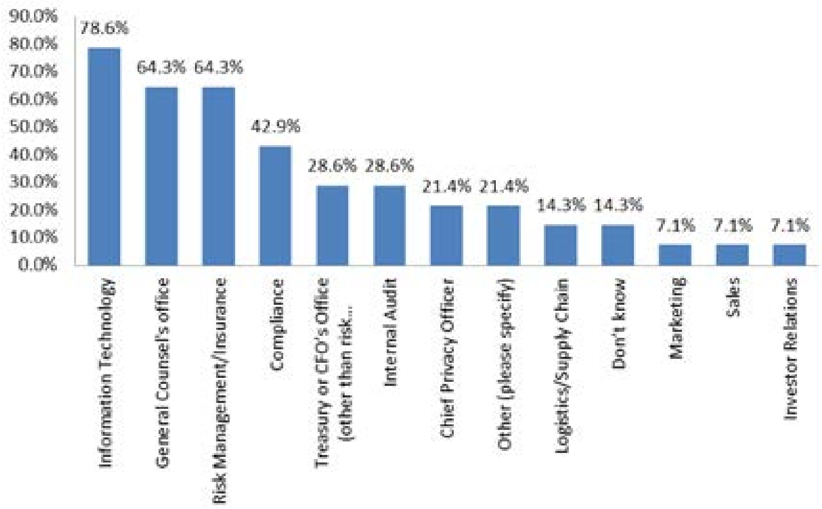
Organisations increasingly include network security risks as part of their risk management focus. Respondents were asked, “Are network security risks a specific risk management focus within your organisation?” 97 percent responded “yes,” and only 3 percent responded “no.” Up 7 percentage points from 2014, this is the fourth consecutive year that the percentage of “yes” responses increased. It has increased a total of 27 percentage points since 2012.

The percentage of respondents who take a multi-departmental approach to their network security risk management efforts fell slightly from 50 percent last year to 45 percent this year. Over the previous two years the U.S. has also experienced a decline in the number of respondents who take a multi-departmental approach. This varies materially, however, based on the size of company with 58 percent of larger companies (turnover of £1 billion or greater) claiming to

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

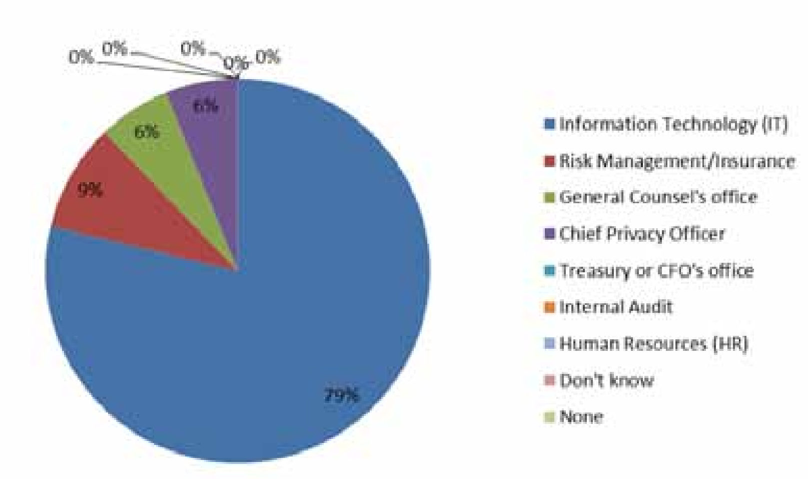
have this team or committee compared with only 13 percent of the smaller companies (turnover under £1 billion). Exhibit 5 illustrates the department or functions that are most likely to have representation on the network security risk management team or committee.

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 defence 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?" 79 percent responded IT with Risk Management/Insurance coming in a distant second with 9 percent. (Exhibit 6)

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



Social media provides businesses with an array of benefits such as increasing brand awareness, promoting products, and providing timely support.

Social Media

Social media provides businesses with an array of benefits such as increasing brand awareness, promoting products, and providing timely support. It also exposes organisations to a degree of risk, such as the potential for reputational damage, privacy issues, infringing others intellectual property, and data breaches. With this in mind respondents were asked, "Does your organisation have a written social media policy?" 75 percent responded "yes." This is identical to the response received in the U.S. survey.

Cloud Services

For a third year respondents were asked questions on cloud services. Thanks to its cost effectiveness and increased storage capacity, cloud services have become a popular alternative to storing data in-house. Warehousing proprietary business information on a third-party server, however, makes some organisations uncomfortable due to the lack of control in securing the information. Nonetheless, security concerns continue to be outweighed by the benefits for a majority of organisations. When asked "Does your company use cloud services?" 61 percent responded "yes," down slightly from 65 percent in 2014. This shift is also apparent in response to the following question, "Is the assessment of vulnerabilities from cloud services part of your data security risk management program?" 59 percent responded "yes," up 6 percentage points from last year.

Mobile Devices

Respondents also were asked questions for a third year on the increasingly important topic of mobile devices. In response to the question "Does your organisation have a mobile device security policy?" 79 percent responded "yes," down slightly from 85 percent last year. Larger companies are more likely to have a mobile device security policy with 83 percent of large companies (turnover £1 billion or greater) responding "yes" compared with 63 percent of smaller companies (turnover £ billion or less). This is a nearly identical response to the U.S. survey.

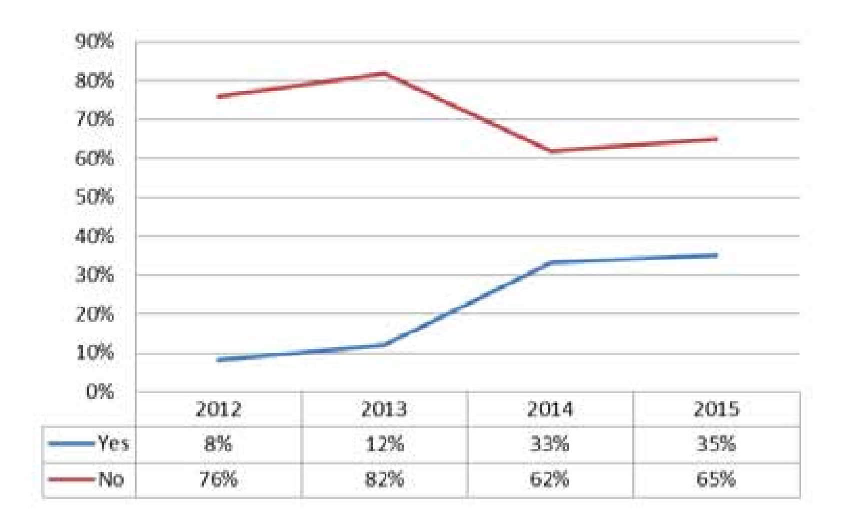
The use of personal handheld devices for business purposes is increasingly preferred by employees and allowed by employers. These non-company controlled devices, however, are accessing proprietary corporate information and frequently exposing organisations to a higher degree of risk. When asked "Does your organisation have a bring your own device (BYOD) policy?" 75 percent responded "yes," a 12 percentage point increase from 2014 and a total of 34 percentage points higher than 2013.

The Role of Insurance in Network Security and Cyber Risk Management

While still significantly below the levels seen in the U.S., the percentage of companies participating in the survey who purchase cyber cover in Europe increased slightly from 33 percent in 2014 to 35 percent this year. (Exhibit 7)

While still significantly below the levels seen in the U.S., the percentage of companies participating in the survey who purchase cyber cover in Europe increased slightly from 33 percent in 2014 to 35 percent this year.

Exhibit 7: Does your organisation purchase cyber liability insurance?



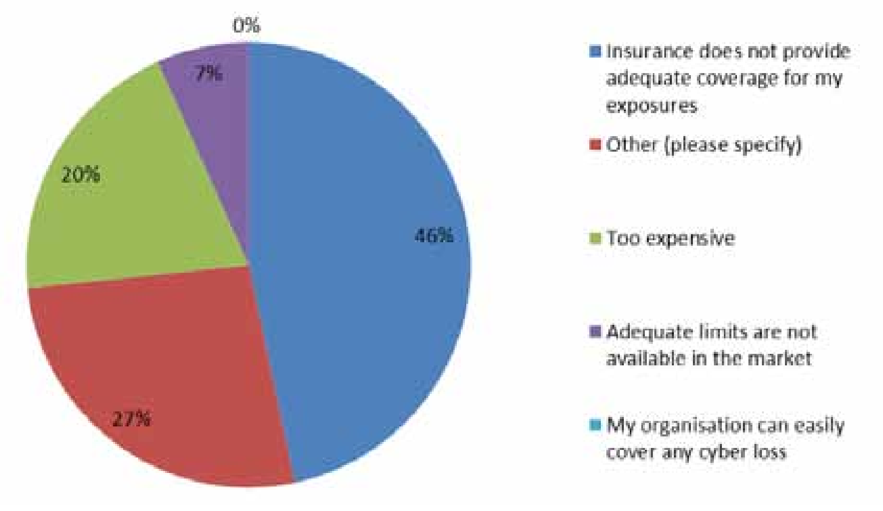
	2012	2013	2014	2015
Yes	8%	12%	33%	35%
No	76%	82%	62%	65%

Of the respondents who purchase coverage, 88 percent said that they have purchased it for less than two years and 13 percent between 3 and five years. None of the respondents have had the coverage for more than five years. The vast majority (88 percent) purchases a stand-alone (mono-line) policy and 13 percent purchase it as part of another policy. None of the respondents have ever had a cyber-insurance claim.

Respondents who do not purchase cyber insurance were asked “Why has your organisation chosen not to purchase cyber insurance?” 47 percent said it is because insurance does not provide adequate coverage for their exposures, 20 percent said it is too expensive, 7 percent said it is because adequate limits are not available in the market, and 27 percent said other. The most common “other” response is that it has not yet been evaluated. (Exhibit 8)

The resounding theme of this year's survey is that while 2014 was chalk full of cyber-related headlines, the network security and cyber liability risk management views and practices have remained relatively consistent from the previous year.

Exhibit 8: Why has your organisation chosen not to purchase cyber insurance?



Organisations 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?" 38 percent respondI thinked "yes," 38 percent "No and 13 percent did not know.

Lastly, respondents were asked for the first time "Is the insurance industry doing enough to address cyber risk with current products?" 26 percent said "yes," 65 percent "No" and 9 percent did not know. As a follow up respondents were asked "In your opinion, how can cyber insurance products be better?" The most common response was providing coverage for a cyber-related property damage event.

Analysis and Conclusions

Collecting data for a fourth consecutive year has further clarified the network security and cyber risk management picture. Trends and practices continue to take shape and marketplace reactions to emerging issues continue to present themselves. Subsequent surveys will help to provide an even stronger reading into this extremely important risk management area.

The resounding theme of this year's survey is that while 2014 was chalk full of cyber-related headlines, the network security and cyber liability risk management views and practices have remained relatively consistent from the previous year. The vast majority of respondents continue to view cyber risks as at least a moderate threat and they continue to be viewed as a significant threat by a majority of executive and board level management.

The nature of cyber security is evolving so quickly it can be difficult for businesses to keep track of the risks let alone the solutions, but this is exactly what businesses today need to do.

Smaller companies continue to view cyber risks less seriously than their larger counterparts; reputational damage remains the biggest concern; IT continues to be responsible for assuring compliance with applicable privacy laws and remains the front line defence against network security risks.

But there are also variances behind the consistency of these broader trends. For example, organisations are more concerned about privacy violations due to a data breach of customer records than in year's past. In addition, network security risks are a specific risk management focus of more organisations but fewer organisations take a multi-departmental approach in addressing these risks.

Nearly the same percentage of companies use cloud services, yet more include the assessment of vulnerabilities from cloud services as part of their data security risk management program. In the same light, while the percentage of companies with a mobile device security policy fell slightly, a significantly higher percentage now has a BYOD policy. Lastly, although cyber risks are perceived as a moderate threat by nearly all organisations, cyber insurance is still not purchased by most but continues to trend in an upward direction.

What can we learn from these behaviours? How is the business community really feeling about the cyber environment and the risk associated with it? Do they truly understand what the threats are and whether they are doing the best they can to protect themselves from these threats?

The nature of cyber security is evolving so quickly it can be difficult for businesses to keep track of the risks let alone the solutions, but this is exactly what businesses today need to do. The insurance industry should be there to help businesses understand what they are facing and what the right solutions are for each of them. ■

This report was written by Josh Bradford, Editor, Advisen Ltd.