ADVISEN
Insurance Intelligence®

2014 NETWORK SECURITY & CYBER RISK MANAGEMENT:

A SURVEY OF ENTERPRISE-WIDE CYBER RISK MANAGEMENT PRACTICES IN THE ASIA-PACIFIC REGION

April 2014

Sponsored by:

ZURICH®

2014 NETWORK SECURITY & CYBER RISK MANAGEMENT:

A SURVEY OF ENTERPRISE-WIDE CYBER RISK MANAGEMENT PRACTICES IN THE ASIA-PACIFIC REGION

Executive Summary

The vast majority of risk professionals, senior executives and board members in the Asia-Pacific region acknowledge that network and information security risks are a threat to their organisations. Most consider the exposures as serious enough to be made the focus of specific risk management activities. Though the level of sophistication in addressing these risks varies widely, the majority prefer to take an enterprise wide – or at least a multi-departmental—approach to addressing the risks. However, under one third of organisations surveyed currently purchase insurance as part of their cyber risk management strategy.

For the first time, 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 the Asia-Pac region.

About the Survey and the Respondents

For the first time, 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 the Asia-Pac region. Conducted for two weeks, the survey began on 10 March, 2014 and concluded on 24 March, 2014. It was completed by 27 risk managers, insurance buyers and other risk professionals.

The largest percentage of respondents (47 percent) classified themselves as Members of Risk Management Departments (Not Head), followed by Other Executive Management (33 percent), Chief Risk Manager/Head of Risk Management Department (15 percent), and IT Manager (5 percent). Respondents with ten years or less of risk management experience represented the largest group at 62 percent of the total, followed by 27 percent with more than 20 years and 12 percent with between 11 – 20 years of experience.

Sponsored by: ZURICH®

The distribution of survey respondents based on the location of their head office is 85 percent Asia/Pacific, 7 percent North America, 4 percent Other Asia, and 4 percent Middle East. The majority of respondents come from multinational enterprises with 31 percent having branches or subsidiaries in 6 – 20 countries, 23 percent in more than 20 countries, 23 percent in 2 – 5 countries, and 15 percent in 1 country. 8 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, Industrials accounts for the largest industry sector with 24 percent of the total respondents; followed by Energy at 16 percent; Banks and Consumer Discretionary both at 12 percent; Healthcare, Materials, Professional Services and Utilities all at 8 percent; and Telecommunications at 4 percent.

Survey responses are evenly distributed based on size with 50 percent of respondents having annual revenues less than $1 billion and 50 percent with revenues greater than $1 billion. Respondents were also asked to provide their employee count. 15 percent have between 501 to 1000 employees, 15 percent between 5,001 to 15,000, 19 percent have more than 15,000, 23 percent less than 500, and 27 percent have between 1,001 to 5,000.

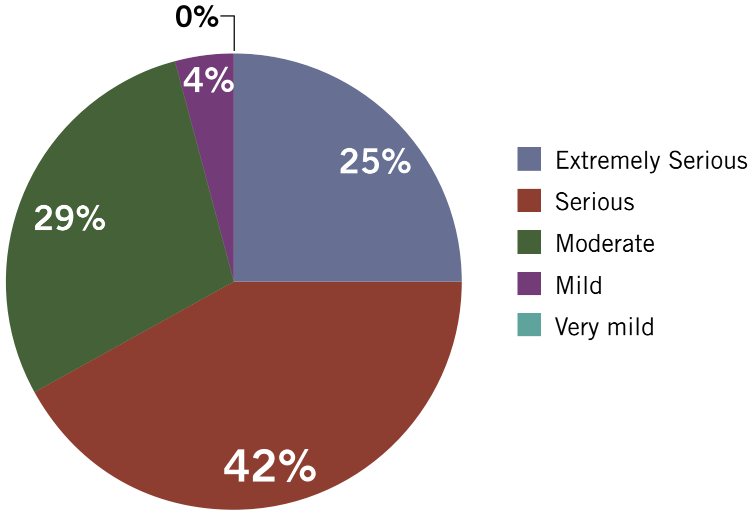
Perception of Cyber Risk

Consistent with similar surveys in North America and Europe, the vast majority of respondents (96 percent) believe that cyber risks pose at least a moderate threat to their organisation.

Consistent with similar surveys in North America and Europe, the vast majority of respondents (96 percent) believe that cyber risks pose at least a moderate threat to their organisation. In response to the question “How would you rate the potential dangers posed to organisation by cyber risks?” 25 percent said extremely serious, 42 percent serious, 29 percent moderate, and 4 percent mild. The 67 percent who believe cyber risks pose a serious or extremely serious threat is slightly lower than in Europe (76 percent) but higher than North America (60 percent). (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?

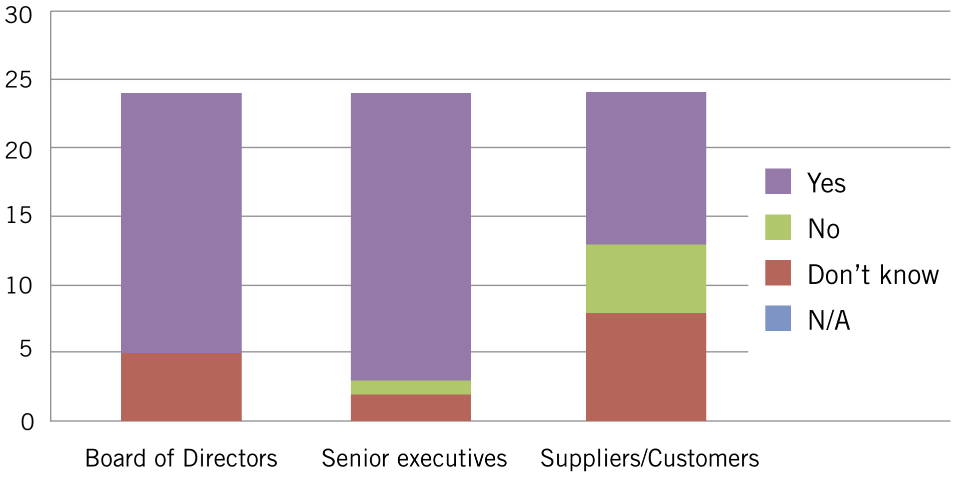


Small and mid-size enterprises (SME) have been shown to be increasingly targeted by cyber criminals. Considered low hanging fruit, SMEs frequently have less sophisticated security and can often act as a conduit to their larger brethren in today's interconnected world. For example, in what is shaping up to be the most costly breaches of all time in United States, it was a heating and air conditioning contractor that reportedly exposed Target Corporation, a leading U.S. retailer, to the breach. However, contrary to the trends identified in Europe and North America where SMEs view cyber threats as much, if not more, seriously than their larger counterparts, this survey revealed the opposite in Asia – Pacific. 86 percent of the largest companies (revenues greater than $5 billion) believe cyber risks pose at least a serious threat to their organisation, compared to only 14 percent of the smallest companies (revenues less than $250 million).

Cyber risks also are viewed as a significant 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: " 79 percent responded yes for Board of Directors (compared with 54 percent in North America and 76 percent in Europe), and 88 percent responded yes for Senior Executives (compared with 64 percent in North America and 71 percent in Europe). Additionally, 46 percent also said that Suppliers/Customers view cyber risks as a significant threat. (Exhibit 2)

In North America the biggest concern was also reputational damage due to a data breach and the lowest concern was theft or loss of customer intellectual property.

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



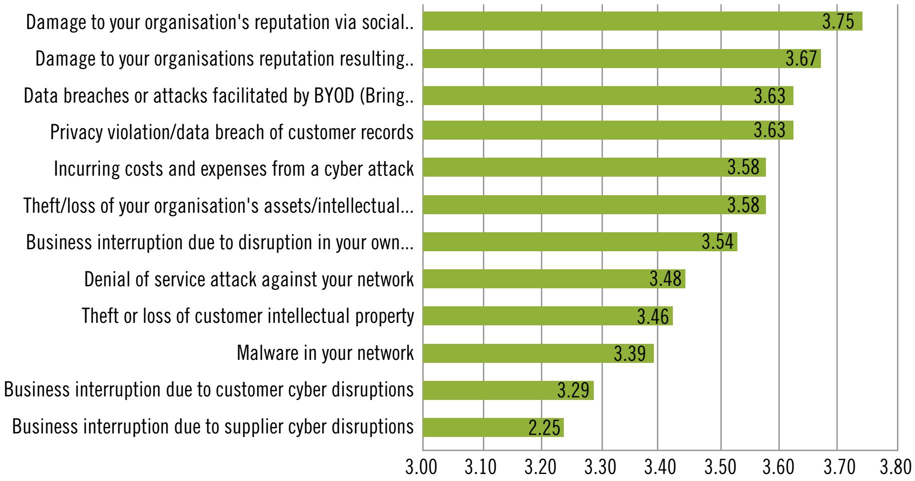
Respondents were asked to rank specified risks on a scale of 1 to 5, with 5 as a very high risk and 1 as a very low risk. Based on the weighted average, the biggest concern of the respondents was damage to their organisation's reputation via social media (3.75), followed by damage to their organisation's reputation resulting from a data breach (3.67). In contrast, the exposures perceived as representing the lowest risks were business interruption due to customer disruptions (3.29) and business interruption due to supplier disruptions (3.25). (Exhibit 3)

For context, in Europe the biggest concern was reputational damage due to a data breach and the lowest was a tie between business interruption due to customer disruptions and employment practices risk due to social media use. In North America the biggest concern was also reputational damage due to a data breach and the lowest concern was theft or loss of customer intellectual property.

Sponsored by: ZURICH®

Businesses and governments with the most sophisticated network security practices and infrastructure often still find they are vulnerable to network breaches.

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



Data Breach Response

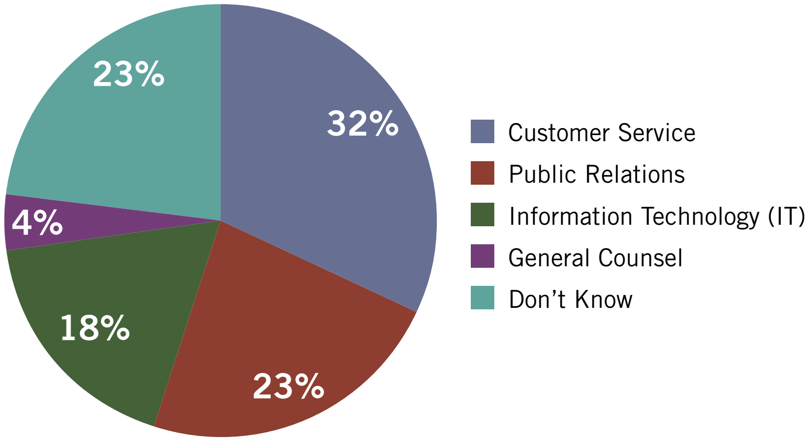
Businesses and governments with the most sophisticated network security practices and infrastructure often still find they are vulnerable to network breaches. For this reason it is recommended that data network breaches be treated as a "when," rather than an "if" proposition. When a breach does occur, research suggests that organisations that have a response plan 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 response plan in place in the event of a cyber-incident?" 70 percent responded yes, 13 percent no, and 17 percent did not know. The 70 percent yes response rate was in line with the North American survey (72 percent) and significantly higher than in Europe (55 percent). Respondents were also asked, "Does your business continuity planning encompass network interruption?" 68 percent responded yes, 5 percent no, and 27 percent do not know. While most claim to be prepared for a cyber-incident against their organisation, far fewer understand the preparedness of their key suppliers. Respondents were asked, "Does your organisation evaluate the network security of your essential suppliers?" 26 percent responded yes, 48 percent no, and 26 percent did not know.

In both North America and in Europe, organisations increasingly include network security risks as part of their risk management focus.

If and when a network security breach occurs, respondents were asked, "In your opinion is your organisation prepared to respond to the data security and privacy laws of all the countries in which you do business?" 65 percent responded yes, 4 percent no, and 30 percent did not know. If it was determined that customers needed to be notified, the department most frequently responsible for the notifications is Customer Service (32 percent), followed by Public Relations (23 percent), Information Technology (IT) (18 percent), and General Counsel (5 percent). 23 percent of respondents did not know. (Exhibit 4)

Exhibit 4: If it is determined that customers be notified of a breach, which department is responsible for the notification?



Information Security and Cyber Risk Management Focus

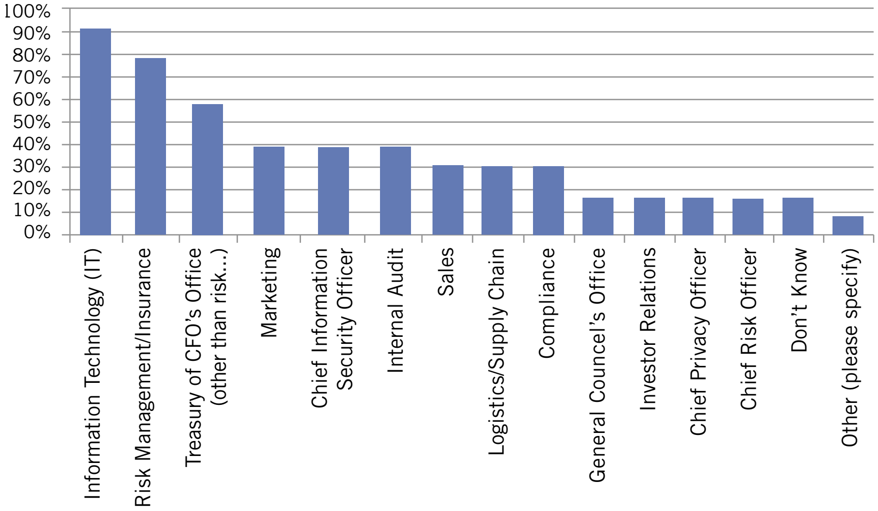
In both North America and in Europe, organisations increasingly include network security risks as part of their risk management focus. With this in mind respondents were asked, "Are network security risks a specific risk management focus within your organisation?" 75 percent said yes, 13 percent no, and the rest did not know. This is lower than in both North America and in Europe where the "yes" responses were 80 percent and 90 percent respectively.

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

The majority of respondents recognise that it is the responsibility of the entire organisation to mitigate network security risks. When asked "does your organisation have a multi-departmental network security risk management team or committee?" 57 percent said yes, 39 percent no, and 4 percent did not know. This is consistent with both the North American and European surveys where 56 percent and 50 percent responded yes respectively. This varies materially, however, based on the size of company with 73 percent of larger companies ($1 billon or greater) claiming to have this team or committee compared with 42 percent of smaller companies (under $1 billion). This is also consistent with the North American and European surveys.

The department or functions most likely to be represented in the network security risk management team are IT with 92 percent and Risk Management/Insurance with 77 percent. (Exhibit 5)

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

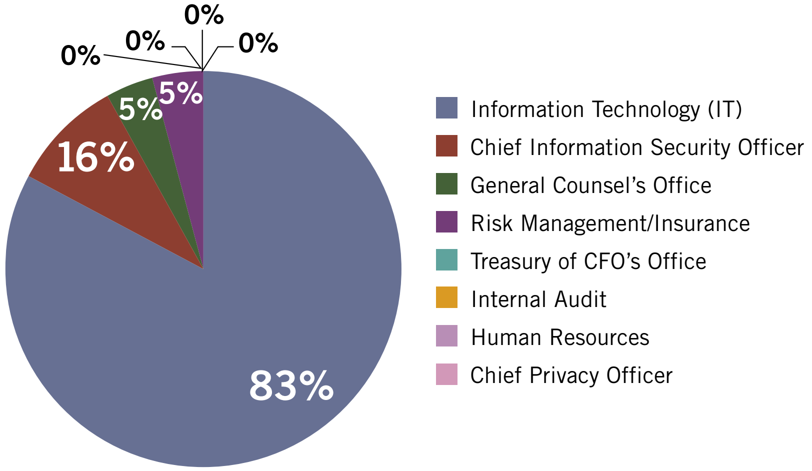


By a wide margin, the IT department is acknowledged as the front line defense against network security risks. In response to the question, "Which department is responsible for leading the information or network security risk management effort?" 83 percent responded IT, 9 percent Chief Information Security Officer and 4 percent for Risk Management and General Counsel. (Exhibit 6)

Sponsored by: ZURICH®

Social media can provide businesses with many benefits such as increasing brand awareness, promoting products or providing timely support.

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 represents 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 consideration. Respondents were asked, "Does your organisation have a written social media policy?" 61 percent responded yes. This is substantially lower than in North America where 76 percent said yes and in Europe where 80 percent said yes.

Mobile Devices and Cloud Computing

Respondents were also asked questions on two increasingly important network security topics, mobile devices and cloud computing. In response to the question, "Does your organisation have a mobile device security policy?" 65 percent said yes. Again, this is lower than in Europe where 85 percent responded yes and North America at 72 percent.

The popularity and extensive capabilities of smartphones has resulted in many employees preferring to use their personal handheld device for business purposes and more and more companies are allowing them to do so. These non-company controlled devices, however, 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?" 39 percent said yes. This is 24 percentage points lower than Europe (63 percent) and 10 percentage points lower than North America.

Although network security risks were widely acknowledged as a concern for the vast majority of organisations, cyber liability insurance is not purchased by most.

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 the U.S. whistleblower Edward Snowden that many of the large cloud service providers such as Google, Apple & Microsoft have complying with the U.S. government's National Security Agency's (NSA) request for specific types of data.

Storing data in the cloud also can raise privacy issues. Regulations sometimes limit where personally identifiable information can be stored, but cloud users often have no idea where their information is physically located.

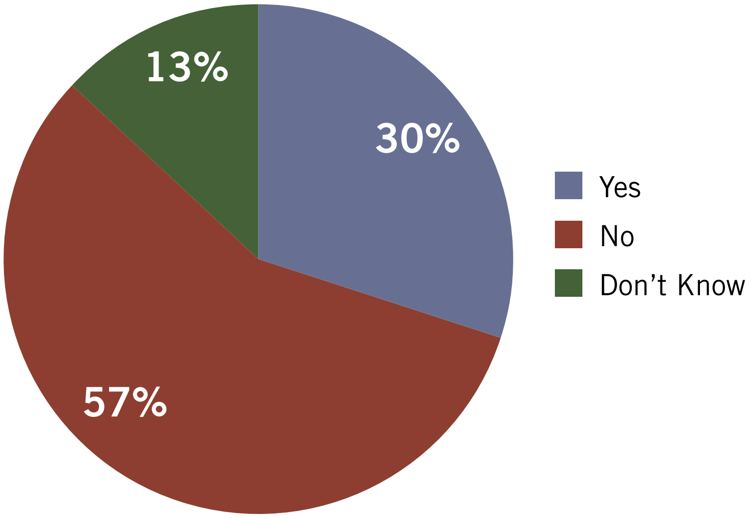
It appears, however, that the benefits of the cloud outweigh much of the risks. When asked, "Does your company use cloud services?" 57 percent responded yes. Respondents were then asked, "Is the assessment of vulnerabilities from cloud services part of your data security risk management program?" 48 percent responded yes.

The Role of Insurance in Network Security and Cyber Risk Management

Although network security risks were widely acknowledged as a concern for the vast majority of organisations, cyber liability insurance is not purchased by most. Survey participants were asked, "Does your organisation buy cyber liability insurance?" 30 percent said yes, 57 percent said no, and 13 percent did not know. (Exhibit 7) Of the respondents who purchase the cover, 29 percent buy a stand-alone (mono line) policy, 57 percent purchase it as a part of another coverage, and 14 percent did not know. Nearly all (86 percent) who purchase cyber insurance also buy coverage for loss of income due to a data breach arising from their network. Finally, those who do not purchase the cover were asked, "Are you considering buying the cover in the next 12 months?" 8 percent said yes, 23 percent no, and 69 percent did not know.

Although there are some differences, many similarities also exist between Asia-Pac companies and companies from the other regions.

Exhibit 7: Does your organisation purchase cyber liability insurance?



Analysis and Conclusions

The first year of this study in the Asia-Pacific region revealed much about the current state of network security and cyber risk management in the region. The baseline has been set, trends in attitudes and practices will begin to take shape and marketplace reactions to emerging issues will emerge. Many of the takeaways from this survey come by way of comparisons to what is taking place in North America and Europe where three consecutive years of data have already been collected. However, subsequent surveys will provide even stronger readings into the trends happening in this increasingly important risk management area in this part of the world.

The theme throughout this survey is that while cyber risks are perceived as a threat by most risk professionals, executive management, and board of directors, Asia-Pac companies have been slower to adopt certain cyber risk management strategies. For example, the threats associated with the use of social media, cloud computing, and mobile devices are less likely to be addressed by Asia-Pac companies than companies in North America and in Europe. Also, cyber threats are still largely perceived as a serious problem by only the largest organisations. In North America and Europe smaller companies now view cyber risks as seriously if not more seriously than their larger counterparts where the opposite is true for Asia-Pac companies.

Although there are some differences, many similarities also exist between Asia-Pac companies and companies from the other regions. For example, a majority of organisations in all regions have some form of multi-departmental network security risk management team or committee with the IT department usually taking the leadership role. IT and risk management also are the departments most likely to have representation in this team across all three regions.

Nearly two thirds of respondents said that their organisations have a data breach response plan in place in the event of a cyber-incident. This is about the same percentage as North America and significantly higher than in Europe. Unlike in North America and Europe, however, where the highest percentage of respondents said the IT department was responsible for assuring compliance with applicable privacy laws, Asia-Pac companies more frequently rely on customer service and public relations to perform this task. This appears to make more sense as IT departments often find that they are ill-equipped to interpret the notification requirements of various countries and jurisdictions.

While most companies claim that network security risks are a specific risk management focus with their organsation, most have not incorporated insurance as part of the strategy.

While most companies claim that network security risks are a specific risk management focus with their organsation, most have not incorporated insurance as part of the strategy. Interest in purchasing the cover also appears to minimal. According to one respondent "I think the product is fairly new in the market, so rather than rushing and buying the product we need to first understand what it actually covers, under what circumstances, and what are the exclusions." ■

This Special Report was written by Josh Bradford, Associate Editor, Advisen Ltd.

About Zurich

Zurich Insurance Group (Zurich) is a leading multi-line insurance provider with a global network of subsidiaries and offices in Europe, North America, Latin America, Asia-Pacific and the Middle East as well as other markets. It offers a wide range of general insurance and life insurance products and services for individuals, small businesses, mid-sized and large companies as well as multinational corporations. Zurich employs about 60,000 people serving customers in more than 170 countries. The Group, formerly known as Zurich Financial Services Group, is headquartered in Zurich, Switzerland, where it was founded in 1872. The holding company, Zurich Insurance Group Ltd (ZURN), is listed on the SIX Swiss Exchange and has a level I American Depositary Receipt program which is traded over-the-counter on OTCQX. Further information about Zurich is available at www.zurich.com.

About Advisen

Advisen generates, integrates, analyzes and communicates unbiased, real-time insights for the global community of commercial insurance professionals. As a single source solution, Advisen helps the industry to more productively drive mission-critical decisions about pricing, loss experience, underwriting, marketing, transacting or purchasing commercial insurance.