ADVISEN
Insurance Intelligence

2013 INFORMATION SECURITY & CYBER LIABILITY & RISK MANAGEMENT

October 2013

Sponsored by:

ZURICH

INFORMATION SECURITY & CYBER LIABILITY & RISK MANAGEMENT:

The Third Annual Survey on the Current State of and Trends in Information Security and Cyber Liability Risk Management

Executive Summary

Historians may look at the year 2013 as a sort of cyber tipping-point – the point at which businesses and governments finally realized the severity of the threats they were facing. Revelations about the NSA's cyber espionage program, evidence of theft of business intellectual property by state-sponsored hackers and attacks on the U.S. financial system by the Syrian Electronic Army are a few of the many cyber events that made headlines.

Exposures such as operational disruptions due to denial of service attacks, lost or stolen data, violation of privacy laws and intellectual property infringement have long been a concern of larger companies. In 2013, smaller businesses began to increasingly realize that they were also at risk. As a result, information security risks became a risk management focus of more organizations and insurance cemented itself as a part of the cyber risk management strategy for a majority of organizations surveyed by Advisen.

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 information security and cyber liability risk management. Conducted for two weeks, the survey began on September 5, 2013 and concluded on September 19, 2013. Invitations to participate were distributed via email to risk managers, insurance buyers and other risk professionals. The survey was completed at least in part by 329 respondents.

The majority of respondents (86 percent) classified themselves as either Chief Risk Mangers/Head of Risk Management Departments (47 percent) or Members of Risk Management Departments (not head) (39 percent). Respondents with more than 20 years of risk management and insurance experience represented the largest group at 42 percent of the total, followed by 29 percent with between 11 - 20 years, 17 percent with between 6 -10 years and 10 percent with 5 years or less.

Businesses from an array of industries are represented. Segmented by 13 macro segments, Healthcare accounts for the largest industry sector with 20 percent of the total respondents; followed by Government and Nonprofit at 12 percent; Industrials at 9 percent; Professional Services, Consumer Discretionary and Utilities all at 8 percent; Non-bank Financial at 7 percent; Education at 6 percent; Banks, Consumer Staples and Energy at 5 percent; Materials at 4 percent; and Telecommunications at 3 percent.

Similar to previous years, the vast majority of respondents (89 percent) believe that cyber and information security risks pose at least a moderate threat to their organization.

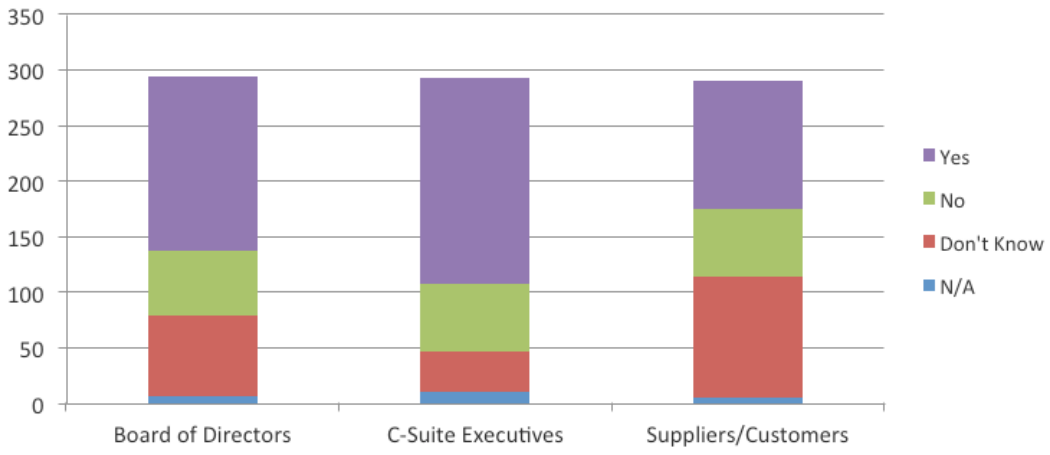
The survey also represents businesses of all sizes but is weighted towards larger companies with 57 percent of respondent companies having revenues in excess of $1 billion. This year respondents also were asked to provide the number of employees. 31 percent have more than 15,000 employees, 25 percent have between 1,001 and 5,000, 22 percent have between 5,001 and 15,000, 12 percent have less than 500 and 11 percent have between 500 and 1,000 employees.

Perception of Cyber Risk

Similar to previous years, the vast majority of respondents (89 percent) believe that cyber and information security risks pose at least a moderate threat to their organization. In last year's report it was noted that while the perception of risk was basically unchanged for risk management and insurance professionals, it was noticeably higher for Board Members and C-Suite Executives. This upward trend in cyber risk perception by Board Members and C-Suite Executives appears to have leveled off. In response to the question "In your experience, are cyber risk viewed as a significant threat to your organization by:" 54 percent said "yes" for board of Directors (52 percent in 2012) and 64 percent said "yes" for C-Suite Executives (65 percent in 2012). (Exhibit 1)

EXHIBIT 1

In your experience, are cyber risks viewed as a significant threat to your organization by:



Small and mid-size businesses can no longer assume that they will be overlooked as a potential target by cybercriminals. In fact, they increasingly are targeted because they often have less sophisticated security and in some cases can act as a conduit to their larger brethren. The 2012 report noted that while the smallest companies (revenues less than $250 million) still viewed cyber risk less seriously than their largest counterparts (revenue greater than $10 billion), the gap is closing.

In response to the question "How would you rate the potential dangers posed to your organization by cyber and information security risks?" 91 percent of smallest companies believe the risks pose at least a moderate danger. This is a 9 percentage point increase from 2012. Conversely, 97 percent of the largest companies believe cyber risks pose at least a moderate danger which was consistent with last year at (96 percent). The percent difference continues to shrink. In 2011, there was an 18 point difference between the percentage of the smallest and largest companies, last year there was a 14 point difference and this year there is only a 6 point difference between the two.

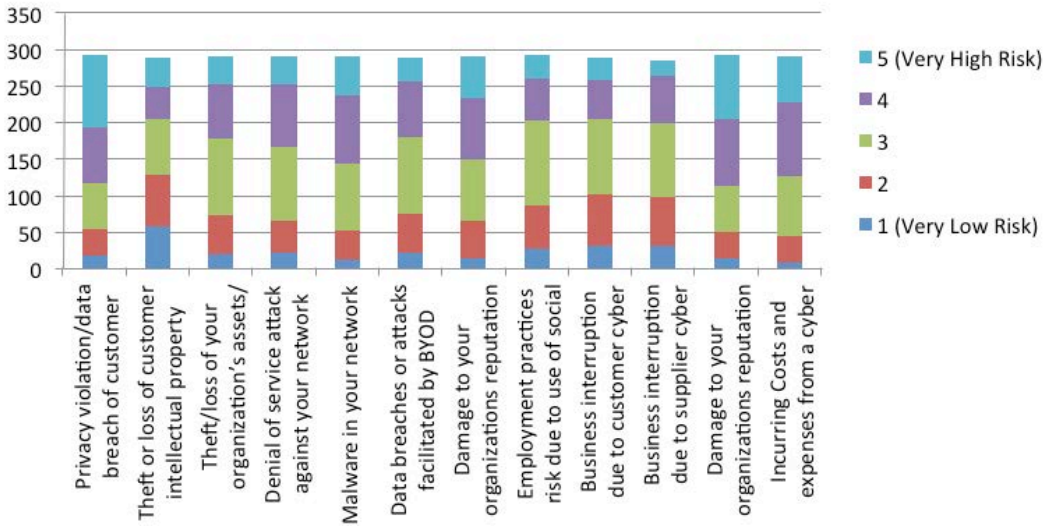
On a scale of one to five, with 5 as very high risk and 1 as very low risk, "damage to your organizations reputation resulting from a data breach" was the biggest concern of respondents, with 61 percent rating it a 4 or 5.

On a scale of one to five, with 5 as very high risk and 1 as very low risk, "damage to your organizations reputation resulting from a data breach" was the biggest concern of respondents, with 61 percent rating it a 4 or 5. This was closely followed by "privacy violation/data breach of customer records" with 60 percent and "incurring costs and expenses from a cyber-attack" at 57 percent.

In contrast, the exposures that were perceived as representing the lowest risks, and had the highest percentage of respondents providing a rating of 1 or 2 included "theft or loss of customer intellectual property" with 45 percent, "business interruption due to customer cyber disruptions" with 36 percent and "business interruption due to supplier cyber disruptions" with 35 percent. (Exhibit 2)

EXHIBIT 2

From the perspective of your organization, 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

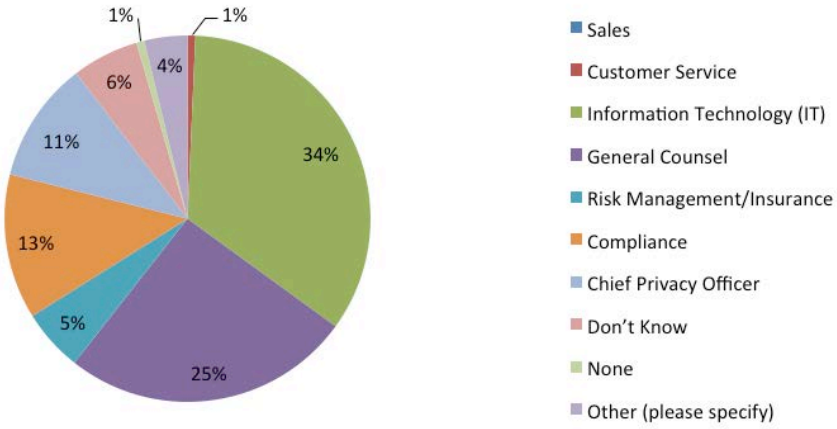
Even businesses or governments with the most sophisticated information security practices and infrastructures are vulnerable to data breaches. For this reason it is recommended that data breaches be treated as a "when," rather than an "if," proposition. When a breach does occur, research suggests that organizations 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 organization have a data breach response plan in place in the event of a data breach?" It appears that most businesses agree with 72 percent responding yes and only 10 percent saying no while 18 percent did not know.

In response to the question "In the event of a data breach, which department in your organization is PRIMARILY responsible for assuring compliance with all applicable federal, state, or local privacy laws including state breach notification laws?" consistent with the previous two surveys, the majority of respondents answered either IT (34 percent) or General Counsel (26 percent). (Exhibit 3)

Information security risks are increasingly a risk management focus. Respondents were asked "Are information security risks a specific risk management focus within your organization?" 80 percent said yes (a 7 percentage point increase from 2012), and 18 percent responded no (a 5 point decline).

EXHIBIT 3

In the event of a data breach, which department in your organization is PRIMARILY responsible for assuring compliance with all applicable federal, state, or local privacy laws including state breach notification laws?



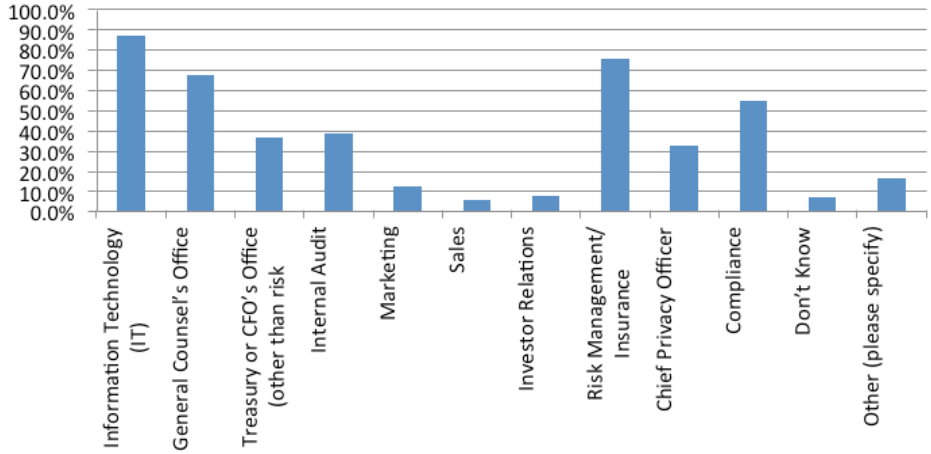
Information Security and Cyber Risk Management Focus

Information security risks are increasingly a risk management focus. Respondents were asked "Are information security risks a specific risk management focus within your organization?" 80 percent said yes (a 7 percentage point increase from 2012), and 18 percent responded no (a 5 point decline). This is especially true for larger organizations with 88 percent of those with revenues in excess of $1 billion responding yes, an increase of 14 percentage points from 2012.

56 percent of organizations have a multi-departmental information security risk management team or committee. This varies materially, however, based on the size of company with 67 percent of larger companies ($1 billion or greater) claiming to have this team or committee compared to only 43 percent of the smaller companies (under $1 billion). The department or functions that are most likely to have representation in the information security risk management team are IT with 88 percent, Risk Management/Insurance 76 percent, General Counsel's Office 68 percent, Compliance 55 percent, Internal Audit 39 percent, Treasury or CFO's Office 37 percent, Chief Privacy Officer 33 percent, Marketing 13 percent, Investor Relations 8 percent and Sales 6 percent (7 percent Didn't Know and 17 percent said Other). (Exhibit 4)

EXHIBIT 4

Which departments are represented on this team or committee?

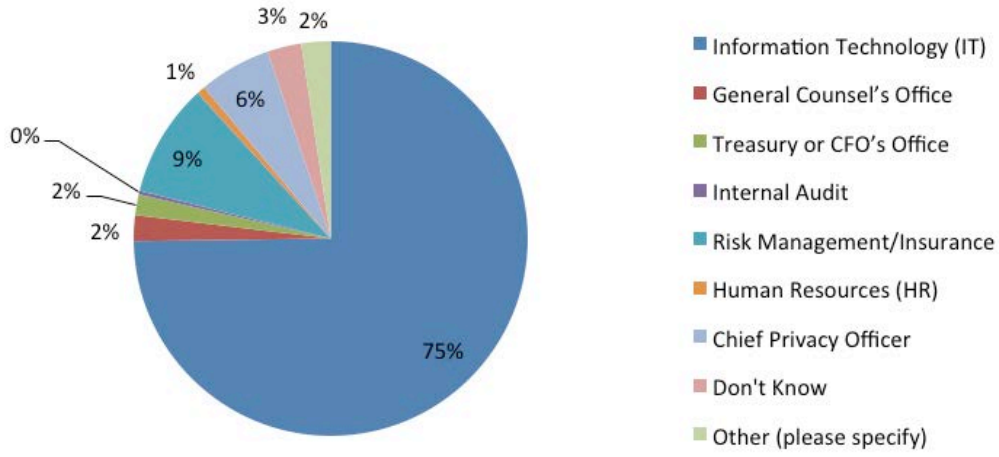


While as a whole the percentage of companies with a mobile device security policy is basically unchanged, the distribution between large a small companies has shifted.

By a wide margin, the IT department is still acknowledged as the front line defense against information losses and other cyber liability risks. In response to the question "Which department is PRIMARILY responsible for spearheading the information security risk management effort?" 75 percent responded IT with Risk Management/Insurance coming in a distant second with 9 percent. (Exhibit 5)

EXHIBIT 5

Which department is PRIMARILY responsible for spearheading the information 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 reputational damage, privacy issues and data breaches. With this in mind respondents were asked "Does your organization have a written social media policy?" Consistent with last year (79 percent) 76 percent responded yes and 15 percent responded no.

Mobile Devices & Cloud Computing

For the second year respondents were asked questions on two increasingly important information security and cyber liability topics, mobile devices and cloud computing. In response to the question "Does your organization have a mobile device security policy?" consistent with last year (75 percent) 72 percent said yes, 15 percent said no and 13 percent did not know. While as a whole the percentage of companies with a mobile device security policy is basically unchanged, the distribution between large a small companies has shifted. Last year there was a 23 percentage point difference between large companies (greater than $1 billion) and smaller organizations. The difference this year is only 4 points, with 74 percent of large companies responding yes and 70 percent smaller companies.

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 organizations to a greater degree of risk. When asked "Does your organization have a bring-your-own device (BYOD) policy?" 49 percent responded yes, a 13 point increase from 2012 confirming that not only are more companies allowing the use of personal devices but they are developing usage policies to mitigate risk.

The upward trend in the percentage of companies purchasing cyber liability insurance protection continued in 2013. For the first time in the three years that this survey has been administered, more than half of the respondents claim to purchase this protection

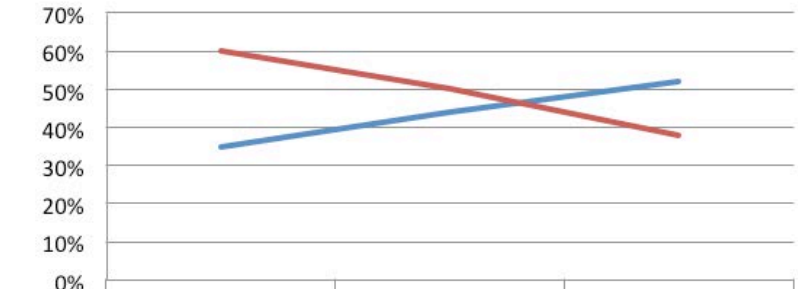
Over the past few years cloud computing has become a popular alternative for businesses seeking to take advantage of its cost effectiveness and increased storage capacity. Warehousing proprietary business information on a third-party server has caused some organizations to question the security of the information being stored. However, the benefits of storing data in the cloud appear to outweigh the risks for more and more organizations. When asked "Does your company use cloud services?" 55 percent responded yes, a 10 point increase from last year. 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?" 53 percent responded yes, up 14 percentage points from last year.

The Role of Insurance in Information Security and Cyber Risk Management

The upward trend in the percentage of companies purchasing cyber liability insurance protection continued in 2013. For the first time in the three years that this survey has been administered, more than half of the respondents claim to purchase this protection. Survey participants were asked "Does your organization purchase cyber liability insurance?" 52 percent responded yes compared to 44 percent in 2012 and 35 percent in 2011. Conversely, 38 percent responded no compared with 50 percent in 2012 and 60 percent in 2011. (Exhibit 6)

EXHIBIT 6

Does your organization purchase cyber liability insurance?



	2011	2012	2013
Yes	35%	44%	52%
No	60%	50%	38%

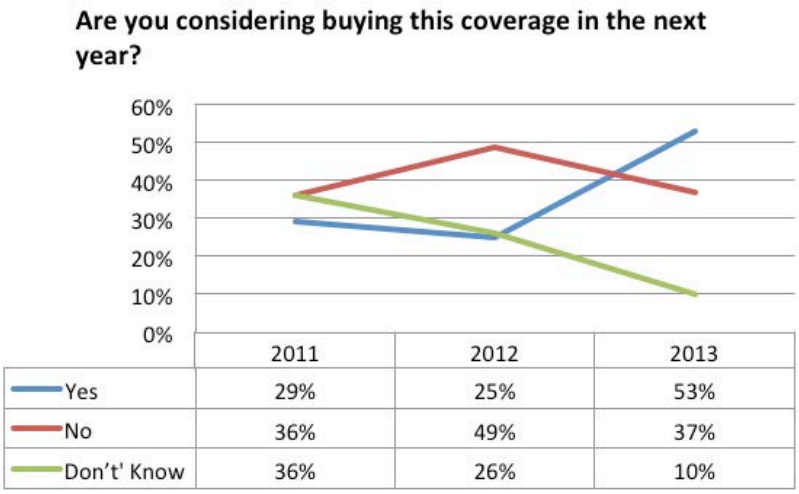
Of the respondents who purchase coverage, 28 percent said that they have purchased it for less than two years, 49 percent between three and five years and 23 percent for over five years. The fact that 72 percent have purchased coverage for more than three years, a 10 point increase from 2012, suggests that when organizations purchase the coverage they see enough value to renew it year after year.

Companies increasingly recognize the business interruption and reputational consequences a data breach may have on their brand. With this in mind, respondents who purchase cyber insurance coverage were asked "Do you currently buy coverage for your loss of income due to data breaches arising from your network?" 54 percent responded yes, 36 responded no and 11 percent did not know.

Respondents that do not currently purchase cyber insurance coverage were asked "Are you considering buying this coverage in the next year?" 53 percent said yes, a 28 percentage point increase from 2012. This is an indication of the continued shift in the cyber insurance marketplace, from a product that was interesting but not a necessity to one that is becoming a must have. (Exhibit 7)

The resounding theme of this year's survey is the increasing concern of small and mid-size businesses over an ever expanding list of information security risks. The gap in the threat perception between the largest and smallest companies is shrinking while the percentage of companies purchasing cyber insurance is substantially increasing.

EXHIBIT 7



	2011	2012	2013
Yes	29%	25%	53%
No	36%	49%	37%
Don't' Know	36%	26%	10%

Analysis and Conclusions

After collecting three consecutive years of data, the information security and cyber liability risk management picture is becoming 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 the increasing concern of small and mid-size businesses over an ever expanding list of information security risks. The gap in the threat perception between the largest and smallest companies is shrinking while the percentage of companies purchasing cyber insurance is substantially increasing. Is this a coincidence or a correlation? Only time will tell but there is clearly an evolving risk landscape along with varying strategies for risk mitigation.

Although the smallest companies increasingly perceive cyber-related risks to be at least a moderate threat, larger companies are still more likely to make it a risk management focus. With this being said, the percentage of organizations with a multi-departmental team focused on data security and privacy remained about the same as last year. While purchasing insurance likely represents the more immediate response to the evolving threat landscape for small and mid-size businesses, moving forward, it will be interesting see if there is a correlation between the implementation of a data security team and the increased perception of cyber related risks.

Finally, small and mid-size businesses also are increasingly concerned with their exposures from mobile devices and employee use of personal devices. Cloud computing is gaining in popularity as businesses of all sizes increasingly perceive the value of storing data in the cloud as outweighing the risks. Not coincidentally, the percentage of organizations that asses the vulnerabilities from cloud services as part of their data security risk management program also increased substantially.