ADVISEN
Insurance Intelligence

SPECIAL REPORT

Information Security and Cyber Liability Risk Management

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

October 2014

ZURICH

Information Security & Cyber Liability Risk Management

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

Executive Summary

If there was any doubt as to the existence of a data security epidemic, 2014 likely changed that. This is the year that it became abundantly clear that no business, government, or individual was immune to the threat of an attack. With massive data breaches affecting some of the nation's largest retailers, nation-states being accused of stealing corporate trade secrets, and private celebrity photos being hacked, 2014 has been chock-full of cyber related headlines.

Cybercriminal tactics continued to evolve and the ability to execute attacks became easier. For many companies, being involved in a cyber event went from a question of "if" to "how bad." Small and midsize businesses increasingly realized that they are highly vulnerable. Information security risks have become a risk management focus for more organizations. Thanks largely to a number of high profile retail breaches, 2014 also has been the year that executives and board members began to view cyber risks more seriously.

About the Survey Respondents

Advisen Ltd and Zurich have partnered for a fourth consecutive year 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 August 5, 2014 and concluded on August 19, 2014. 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 507 respondents.

The majority of respondents classified themselves as either Member of Risk Management Department (not head) (38 percent) or Chief Risk Manager/Head of Risk Management Department (33 percent). Respondents with more than 20 years of risk management and insurance experience represented the largest group at 39 percent of the total, followed by 25 percent with between 11 – 20 years, 18 percent with 5 years or less, and 17 percent with between 6 – 10 years.

Respondents' perception of cyber risk is largely unchanged from last year with 88 percent considering cyber and information security risks to be at least a moderate threat to their organization. Respondents do however believe that board members and executive management are viewing cyber risks more seriously.

Businesses from an array of industries are represented. Segmented by 13 macro segments, Healthcare accounts for the largest industry sector with 16 percent of the total respondents; followed by Government and Nonprofit and Professional Services both at 13 percent; Consumer Discretionary and Industrials at 9 percent; Nonbank Financial at 8 percent; Consumer Staples, Education, Energy, Materials, and Utilities all at 5 percent; Banks at 4 percent; and Telecommunications at 3 percent.

The survey also represents businesses of all sizes, but is weighted towards larger companies with 55 percent of respondent companies having revenues in excess of $1 billion. In terms of employees, 24 percent have between 5, 000 and 15,000 employees, another 24 percent have more than 15,000 employees, 23 percent have between 1,001 and 5,000, 21 percent have less than 500, and 8 percent have between 500 and 1,000 employees.

Perception of Cyber Risks

Respondents' perception of cyber risk is largely unchanged from last year with 88 percent considering cyber and information security risks to be at least a moderate threat to their organization. Respondents do however believe that board members and executive management are viewing cyber risks more seriously. In response to the question "In your experience, are cyber risks viewed as a significant threat to your organization by:" 64 percent said "yes" for Board of Directors (54 percent in 2013) and 72 percent said "yes" for C-Suite Executives (64 percent in 2013).

Exhibit 1:

Although studies have suggested that small companies are targeted as frequently, if not more so, than larger companies, as a group they continue to view cyber risks less seriously.

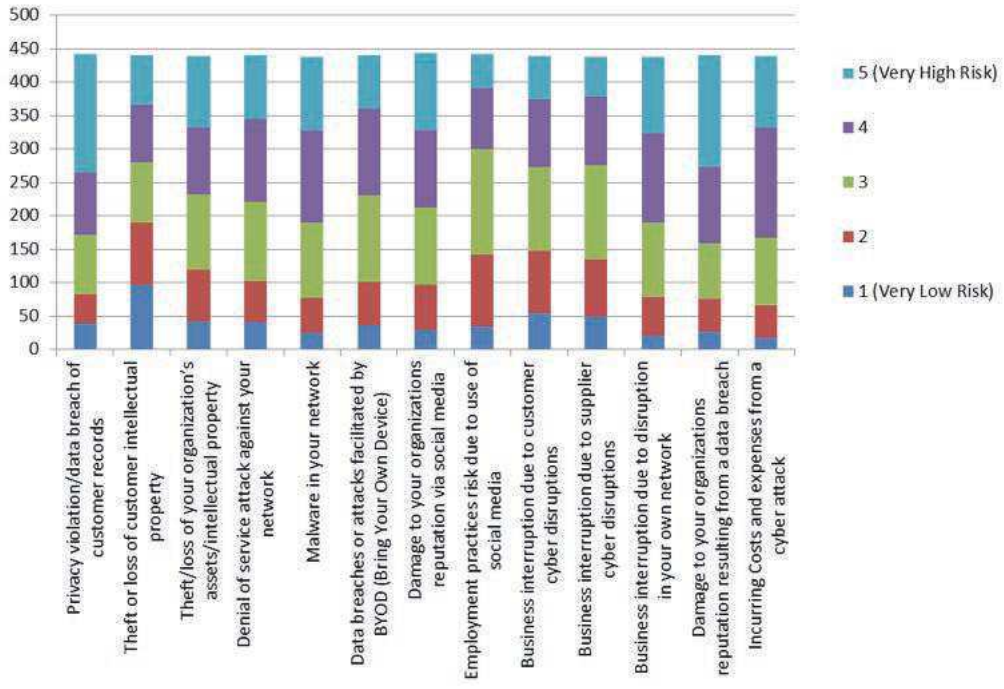
Perception of risk varies based on size of business. Although studies have suggested that small companies are targeted as frequently, if not more so, than larger companies, as a group they continue to view cyber risks less seriously. In response to the question "How would you rate the potential dangers posed to your organization by cyber and information security risks?" 81 percent of the smallest companies (revenues less than $250 million) consider cyber risks to be at least a moderate danger while 93 percent of the largest companies (revenue greater than $10 billion) consider them to be so.

Consistent with last year's study, on a scale of one to five, with 5 as very high risk and 1 as very low risk, "damage to your organization's reputation resulting from a data breach" is the biggest concern of respondents with 64 percent rating it a 4 or 5. This was closely followed by "incurring costs and expenses from a cyber-attack" with 62 percent, and "privacy violation/data breach of customer records" with 61 percent.

In contrast, the exposure perceived as the least risky was "theft or loss of customer intellectual property" with 43 percent rating it a 1 or 2. This was followed by "business interruption due to customer cyber disruptions" with 33 percent, and "employment practice risk due to use of social media" with 32 percent.

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.



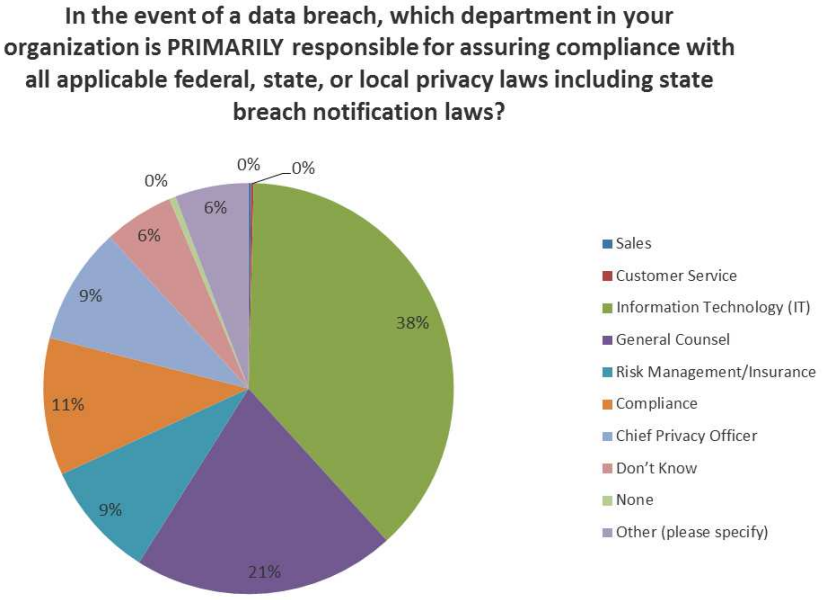
Data Breach Response

Some suggest that corporate data breaches are no longer an "if" or even a "when" proposition, but rather "how bad" will the inevitable breach be.

Over the past year, huge and highly recognizable U.S. businesses have fallen victim to some of the largest data breaches in history. These breaches are proof that even those with the most sophisticated information 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" will the inevitable breach be. When a breach does occur, research suggests that organizations that have data breach response plans in place prior to a breach, fare much better than those who do not. It was with this in mind that respondents were asked "Does your organization have a data breach response plan in the event of a data breach?" Sixty-two percent said yes, 14 percent said no, and 24 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 will previous surveys, IT (38 percent) and General Counsel (21 percent) received the highest percentage of the responses.

Exhibit 3:



Information Security and Cyber Risk Management Focus

For a second consecutive year, the percentage of respondents with a multi-departmental information security risk management team or committee has declined.

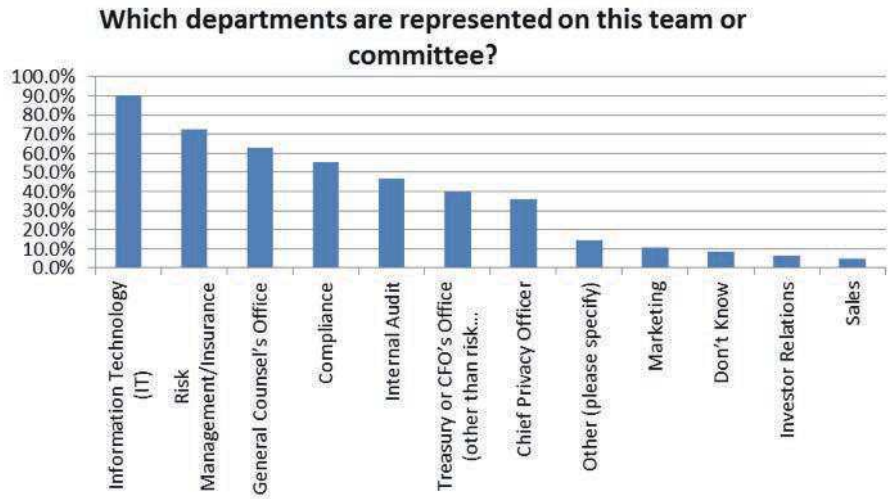
Consistent with the 2013 survey, the vast majority of respondents (80 percent) claim that information security risks are a specific risk management focus within their organization. Larger companies are slightly more likely to make it a focus with 83 percent of companies with revenues in excess of $1 billion doing so, compared with 77 percent with revenues under $1 billion. However, the six percentage point difference between small and large companies is significantly less the 17 point difference from a year ago.

The difference is even more significant when comparing the largest companies (revenues of $10 billion or greater) and the smallest companies (revenues of $250 million or less), with 92 percent of the largest companies making information security a risk management focus compared with only 72 percent of the smallest companies.

For a second consecutive year, the percentage of respondents with a multi-departmental information security risk management team or committee has declined. This year, 52 percent have an information security risk management team or committee which is down from 56 percent in 2013, and 61 percent in 2012. Although statistically still within the margin of error, this is a potential trend worth following. As in previous years, however, this varies materially based on the size of company with 58 percent of larger companies ($1 billion in revenue or greater) claiming to have this team or committee compared to 42 percent of smaller companies (under $1 billion in revenue).

The departments most likely to have representation on the information security risk management team are IT with 90 percent, Risk Management/Insurance (73 percent), General Counsel (63 percent), Compliance (55 percent), Internal Audit (47 percent), Treasury or CFO's Office (40 percent), Chief Privacy Officer (36 percent), Marketing (10 percent), Investor Relations (6 percent), and Sales (5 percent). Nine percent Didn't Know and 15 percent said Other. The most common write-in responses under "Other" were Operations and Security.

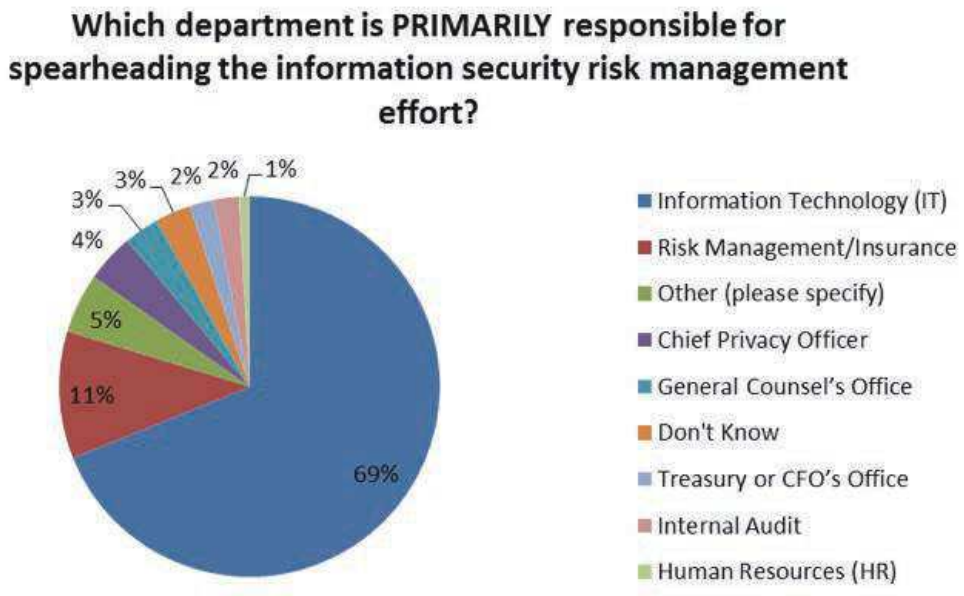
Exhibit 4:



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

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?" 69 percent responded IT with Risk Management/Insurance coming in a distant second with 11 percent. Five percent responded Other, with the most common write-in response being Information Security.

Exhibit 5:



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 organizations to a degree of risk, such as the potential for reputational damage, privacy issues, infringing other intellectual property, and data breaches. With this in mind respondents were asked "Does your organization have a written social media policy?" In line with previous surveys, 74 percent responded yes and 17 percent no.

Cloud Services

For a third consecutive 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 organizations uncomfortable due to the lack of control in securing the information. Nonetheless, security concerns continue to be outweighed by the benefits. When asked "Does your company use cloud services?" 66 percent responded yes, up from 55 percent last year, and 45 percent in 2012. As a follow up, respondents were asked "Is the assessment of vulnerabilities from cloud services part of your data security risk management program?" consistent with last year 51 percent responded yes.

The upward trend in the percentage of companies purchasing cyber liability insurance plateaued in 2014.

Mobile Devices

Respondents were also asked questions for a third year on the increasingly important topic of mobile devices. In response to the question "Does your organization have a mobile device security policy?" consistent with the previous two years, 74 percent said yes, 15 percent said no, and 13 percent did not know. Larger companies continue to be more likely to have such a policy with 82 percent of large companies ($1 billion or greater) responding yes compared with 62 percent of smaller companies ($1 billion or less).

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 organizations to a higher degree of risk. When asked "Does your organization have a bring your own device (BYOD) policy?" 47 percent responded yes which is consistent with last year's response.

The Role of Insurance in Information Security and Cyber Risk Management

The upward trend in the percentage of companies purchasing cyber liability insurance plateaued in 2014. Survey participants were asked "Does your organization purchase cyber liability insurance?" 52 percent responded yes, 35 percent said no, and 13 percent did not know.

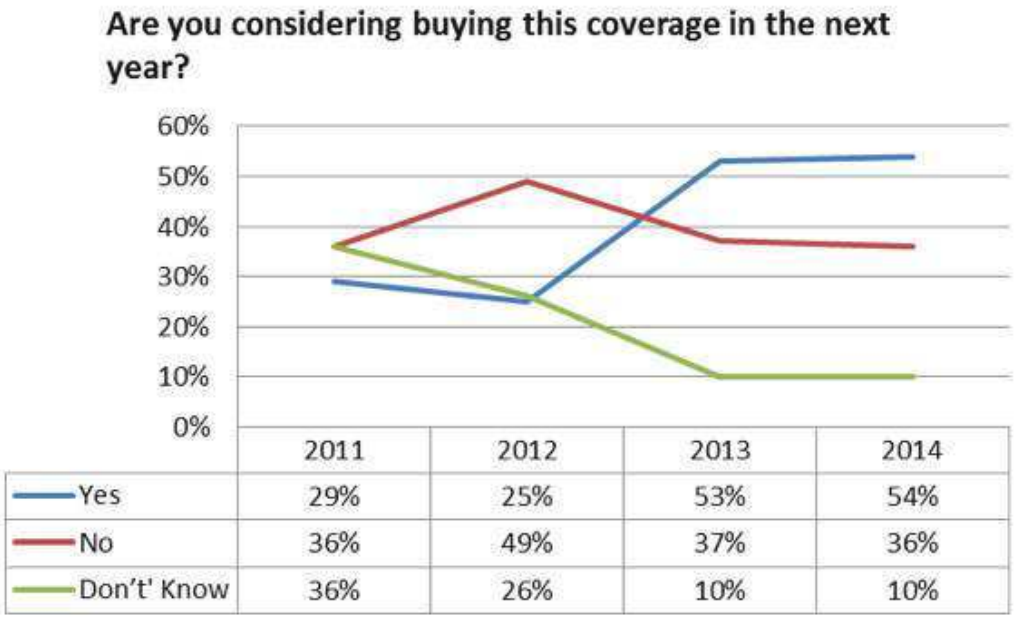
Exhibit 6:

Of the respondents who purchase coverage, 32 percent have purchased it for less than two years, 47 percent between three and five years, and 22 percent for more than five years.

Of the respondents who purchase coverage, 32 percent have purchased it for less than two years, 47 percent between three and five years, and 22 percent for more than five years. Additionally, the percentage of companies who buy coverage for loss of income due to a data breach dropped slightly from 54 percent in 2013 to 48 percent this year.

Finally, respondents that do not currently purchase cyber insurance were asked "Are you considering buying this coverage in the next year?" 54 percent said yes. This was only a one percentage point increase from 2013.

Exhibit 7:



	2011	2012	2013	2014
Yes	29%	25%	53%	54%
No	36%	49%	37%	36%
Don't' Know	36%	26%	10%	10%

Analysis and Conclusions

Collecting data for a fourth consecutive year has further clarified the information security and cyber risk management picture. Trends and attitudes 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 seemingly endless stream of cyber-related headlines in 2014 that included some of the largest data breaches in U.S. history opened the eyes of many businesses as to the true threat to their operations, reputation, customers and their bottom line. As a result, consumer backlash is growing and businesses are reeling from damaged reputations and the costs associated with breach response and legal defense. Interestingly, amongst all of this cyber-related activity, information security and cyber liability risk management views and practices have remained relatively consistent from the previous year.

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 that is exactly what businesses today need to do.

The vast majority of respondents continue to perceive information security risks as at least a moderate threat; smaller companies continue to view cyber risks slightly less seriously than their larger counterparts; larger companies remain more likely to make information security a specific risk management focus; reputational damage remains the biggest concern; IT and General Counsel continue to be responsible for assuring compliance with privacy laws; and IT is still the front line defense against information security risks.

But there are also variances behind the consistency of these broader trends. For example, although the respondents' view of information security risks is unchanged, executives and the board members are viewing cyber risks more seriously. And although larger companies are more likely to make information security a specific risk management focus, the difference between the percentage of small companies and large companies who do so is closing.

The data also points to a potential shift in terms of how organizations are addressing these risks. While information security remains a focus of most organizations, for a second consecutive year there was a decrease in the percentage of companies with a multi-departmental information security team or committee. A decline was also evident in terms of the percentage of companies that have a data breach response plan in place. These results are even more surprising given the sizeable increase since last year of Board and C-suite executives who view cyber risk as a significant threat to their organizations.

More companies are using cloud services, yet the same percent of companies responded that the assessment of vulnerability from cloud services is part of organization's data security risk management program. In the same light, nearly 50 percent of companies have instituted "Bring Your Own Device" policies, which increase exposure to a higher degree of risk. Lastly, and maybe most startling, the number of organizations who purchase cyber insurance plateaued.

What can we learn from these behaviors? How is the business community really feeling about the cyber environment and the risks 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 that is exactly what businesses today need to do.

And the insurance industry should be there to help them 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.