Advisen
Transforming • Insurance™

INFORMATION SECURITY AND CYBER LIABILITY RISK MANAGEMENT

THE FIFTH ANNUAL SURVEY ON THE CURRENT STATE OF AND TRENDS IN INFORMATION SECURITY AND CYBER LIABILITY RISK MANAGEMENT

Sponsored by

ZURICH®

October 2015

TABLE *of* CONTENTS

3 EXECUTIVE SUMMARY

3 KEY FINDINGS

3 ANALYSIS AND CONCLUSIONS

4 PERCEPTION OF CYBER RISK

7 DATA BREACH PREPARATION

- SOCIAL MEDIA
- MOBILE DEVICES
- CLOUD SERVICES
- INTERNET OF THINGS (IOT)

10 INFORMATION SECURITY AND CYBER RISK MANAGEMENT FOCUS

12 THE ROLE OF INSURANCE

15 ABOUT THE SURVEY RESPONDENTS

ZURICH® Advisen Transforming Insurance

EXECUTIVE SUMMARY

A quote provided by a respondent to this year's survey captures the mindset of many risk professionals in 2015: "You can never be too prepared. It can happen in many ways… You have to always be on guard and educated."

With devastating data breaches affecting organizations of all sizes and in all industries, cyber risks are a growing concern that requires an enterprise-wide approach to risk management. Increased cyber risk focus from boards and senior executives may translate into strategic cyber prevention and response initiatives in more organizations. Exposures such as a data breach of customer records and reputational damage resulting from a data breach are high on the list of concerns.

MORE ORGANIZATIONS ARE LOOKING AT INSURANCE AS A KEY COMPONENT OF THEIR OVERALL CYBER RISK MANAGEMENT STRATEGY.

As a result, more organizations are looking at insurance as a key component of their overall cyber risk management strategy. "After a few missed opportunities spanning about four years, we have finally purchased a cyber risk insurance policy," explained one risk professional. "Risk management was always concerned about the risk, and now our board and officers are concerned in light of all the events that have occurred."

KEY FINDINGS

- The overall upward trend of organizations purchasing cyber liability insurance accelerated in 2015.
- Two-thirds of respondents have either increased their policy limits or are considering increasing their limits. The vast majority of respondents purchase cyber coverage on a standalone basis.
- Organizations are increasingly developing data breach response plans.
- Organizations are increasingly concerned with the security of non-company controlled mobile devices.
- The primary reason why respondents have yet to purchase coverage is that their superiors do not see the need.
- Risk professionals increasingly view cyber risks as an extremely serious threat.
- Boards and executive management continue to view cyber risks more seriously.
- Privacy violation/data breach of customer records is the biggest concern of respondents.
- Three quarters of surveyed organizations have a key executive with oversight responsibility or whose main focus is cybersecurity.
- More organizations view information security as an organizational challenge rather than just an issue to be addressed by the Information Technology (IT) department.
- IT is the most represented department on information security risk management teams or committees and is responsible for leading the effort in most organizations.

ANALYSIS AND CONCLUSIONS

"As the company risk manager, I believe cyber liability is an insurance need just like auto, general liability and property."

This quote by a survey respondent is indicative of the evolution in corporate mindset over the past five years regarding information security and cyber liability. In 2011, cyber insurance was still a novelty to many risk managers, and relatively few companies bought the cover. In 2015, more than 60 percent of companies participating in the survey are insured. Five consecutive years of data demonstrate how attitudes have changed and how the marketplace reacts to emerging issues.

In 2011, cyber insurance was still a novelty to many risk managers, and relatively few companies bought the cover. In 2015, more than 60 percent of companies participating in the survey are insured.

The vast majority of respondents continue to perceive cyber risks as at least a moderate threat, and more organizations are viewing it as an extremely serious threat. Large organizations on average perceive the threat as greater than smaller organizations. That may be a reason why smaller companies are less likely to allocate resources to cybersecurity. "It's a growing concern, but limited resources to address leave us vulnerable," wrote a respondent. "I continue to raise the issue. Coverage continues to develop. Hopefully we will be looking at conducting a retention/transfer plan in the upcoming year."

One trend that has significant implications for how organizations prepare and respond to the evolving cyber risk landscape is the increased attention paid by boards and executive management to cyberrelated issues. The issues of greatest concern, however, have remained fairly consistent throughout the years with data/privacy breaches of customer records and reputational damage consistently at the top of the list.

While the issues of concern have held constant, how organizations prepare for and respond to cyber incidents is evolving. Organizations are becoming increasingly proactive in developing data breach response plans to mitigate the severity of a loss. For example, "The cyber liability exposure is now the organization's fourth largest concern. We are conducting analytics to assess our security gaps and implementing a response plan. In the very near future, we will begin implementing ISO 22301 and ISO 27001," said one respondent.

Additionally, organizations are assigning a key executive such as a Chief Information Officer (CIO) or Chief Information Security Officer (CISO) with cybersecurity oversight responsibility. They are also viewing cybersecurity as an enterprise-wide issue that requires a multi-departmental approach.

The level of attention paid to social media and cloud services exposure remained consistent with previous surveys. Mobile devices (both company issued and BYOD), however, are receiving increased attention.

The Internet of Things (IoT) is an emerging risk that is only now beginning to gain awareness among risk managers. In this year's survey, the percentage of respondents who knew whether their organizations were at risk was nearly equal to the percentage who did not know if they were exposed. As the IoT becomes more prevalent and more people understand how it impacts their businesses, it is fair to assume this exposure may be top of mind for more organizations in future surveys.

Lastly, the percentage of organizations that purchase cyber liability insurance as a component of their overall cyber risk management program jumped in 2015, and more organizations are considering purchasing the coverage in the coming year.

But challenges still remain. "It's so difficult to get your hands around what a potential loss may be in order to make informed decisions around the purchase of coverage," said one respondent. "This area scares me to death, and I struggle with how we can best manage it," accrding to another. "Cyber liability insurance can certainly help, but the limits that are needed seem to be very expensive especially for a small organization like ours. I hope to make a decision this year about cyber liability insurance and what limits."

PERCEPTION OF CYBER RISKS

Cyber risks continue to be viewed as at least a moderate threat by the vast majority of risk professionals. This year, 92 percent said cyber risks pose at least a moderate threat to their organization, a five percentage point increase

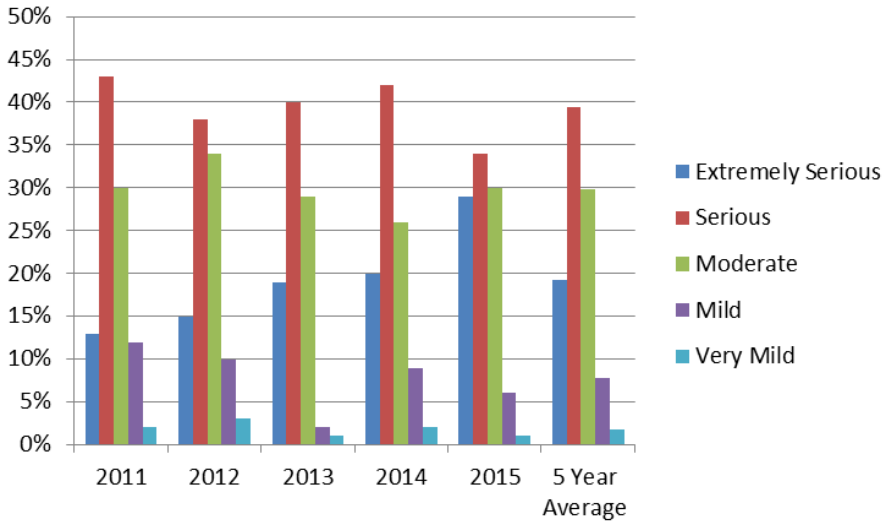
THE LEVEL OF CONCERN, HOWEVER, IS INCREASING. TWENTY-NINE PERCENT SAID CYBER RISKS POSE AN EXTREMELY SERIOUS THREAT TO THEIR ORGANIZATION, UP FROM 20 PERCENT IN 2014 AND A TOTAL OF 16 PERCENT SINCE 2011.

from the previous year and 4 percentage points above the five year average of 88 percent.

The level of concern, however, is increasing. Twenty-nine percent said cyber risks pose an extremely serious threat to their organization, up from 20 percent in 2014 and a total of 16 percent since 2011. (Exhibit 1)

EXHIBIT 1:

How would you rate the potential dangers posed to your organization by cyber & information security risks?



Company size may influence cyber risk perception. 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 risk less seriously. For example, this year 30 percent of the smallest companies (revenues less than $250 million) rate the potential dangers posed to their organization by cyber risks as extremely serious compared with 52 percent of the largest companies (revenue greater than $10 billion).

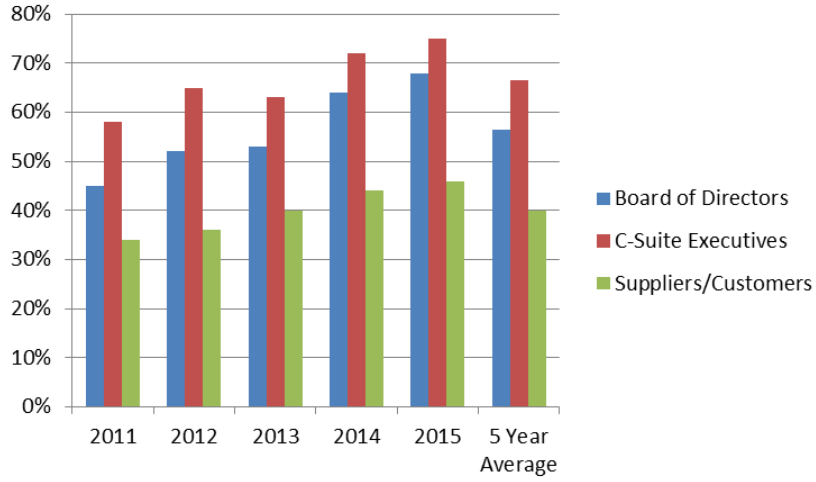
Boards and executive management also continue to view cyber risks more seriously. In response to the question, “In your experience, are cyber risks viewed as a significant threat to your organization?” 68 percent said yes for Board of Directors, 4 percentage points higher than in 2014 and 23 percentage points higher than the first survey in 2011.

Seventy-five percent said yes for C-Suite Executives, 3 percentage points higher than 2014 and 17 points higher than the first survey in 2011. (Exhibit 2)

Boards and executive management also continue to view cyber risks more seriously. In response to the question, “In your experience, are cyber risks viewed as a significant threat to your organization by:” 68 percent said yes for Board of Directors, 4 percentage points higher than in 2014 and 23 percentage points higher than the first survey in 2011.

EXHIBIT 2:

In your experience, are cyber risks viewed as a significant threat to your organization by: (Graph illustrates "yes" responses only)

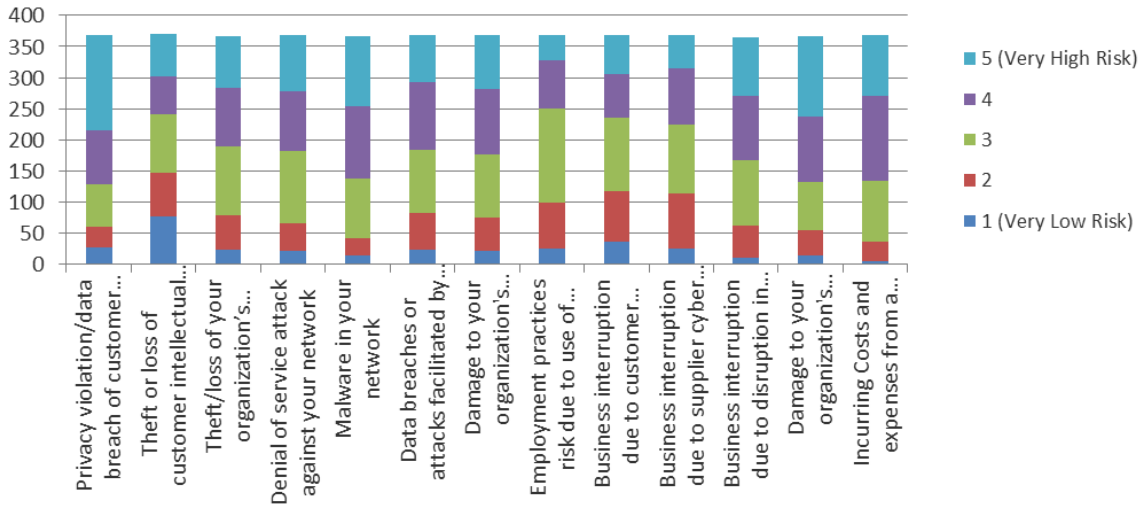


On a scale of one to five, with 5 as very high risk and 1 as very low risk, "Privacy violation/data breach of customer records" is the biggest concern of respondents with 65 percent rating it a 4 or 5. This replaced "damage to your organization's reputation resulting from a data breach," which held the top spot the previous two years but still remains a significant concern with 64 percent rating it a 4 or 5. "Incurring costs and expenses from a cyberattack" rounded out the top three also with 64 percent, rating it a 4 or 5.

In contrast, the exposure perceived as the least risky remained "theft or loss of customer intellectual property" with 40 percent of respondents rating it a 1 or 2, followed by "business interruption due to customer cyber disruptions" with 32 percent and "business interruption due to supplier cyber disruptions" with 31 percent. (Exhibit 3)

EXHIBIT 3:

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 PREPARATION

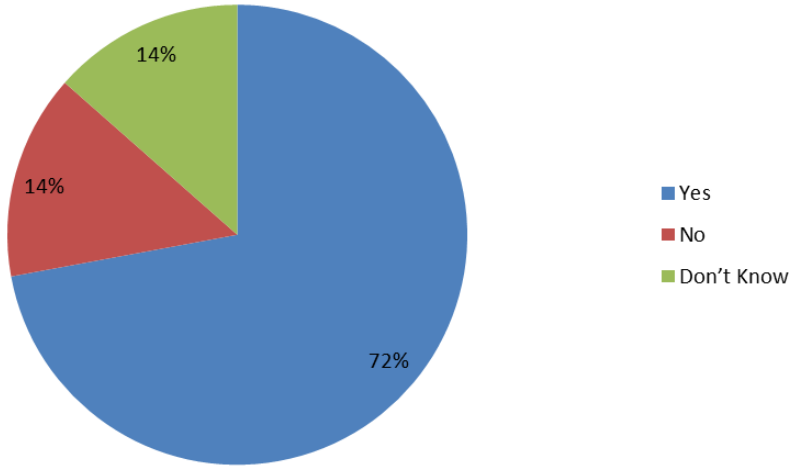
Major U.S. businesses, as well as departments in both federal and state governments, continue to report some of the largest data breaches in history. Frequent penetration of highly fortified networks is evidence that even the most sophisticated cybersecurity infrastructures can be overcome by highly motivated criminals or state-sponsored actors. As a result, cybersecurity strategies are evolving as more organizations realize that perimeter defenses alone may not be sufficient.

With more risk professionals and senior leaders viewing cyber risk as a significant threat, a greater focus has been put on preparation in effort to minimize exposures. For example, respondents were asked, "Does your organization have a data breach response plan in place in the event of a data breach?" Seventy-two percent responded yes, an increase of 10 percentage points from 2014. (Exhibit 4)

WITH MORE RISK PROFESSIONALS AND SENIOR LEADERS VIEWING CYBER RISK AS A SIGNIFICANT THREAT, A GREATER FOCUS HAS BEEN PUT ON PREPARATION IN EFFORT TO MINIMIZE EXPOSURES.

EXHIBIT 4:

Does your organization have a data breach response plan in place in the event of a data breach?



Preparation requires an understanding of changing exposures. One area that continues to rapidly evolve is the increasing reliance on technology for various business functions. Although technology often increases productivity and efficiency, it can also expose an organization to heightened data security risks. With this in mind, respondents were asked a series of questions on technology such as social media, mobile devices, cloud services and the Internet of Things (IoT).

SOCIAL MEDIA

Social media provides businesses with an array of benefits such as increasing brand awareness, promoting products and providing timely support. It may also expose organizations to risks such as reputational damage, privacy issues, intellectual property infringement and data breaches. With this in mind, respondents were asked, "Does your organization have a written social media policy?" In line with previous surveys, 76 percent of respondents said yes.

MOBILE DEVICES

Another challenge facing corporate IT departments is securing both privately owned and corporate issued mobile devices. Educating users on the data security threats offered by these devices can help to significantly reduce their

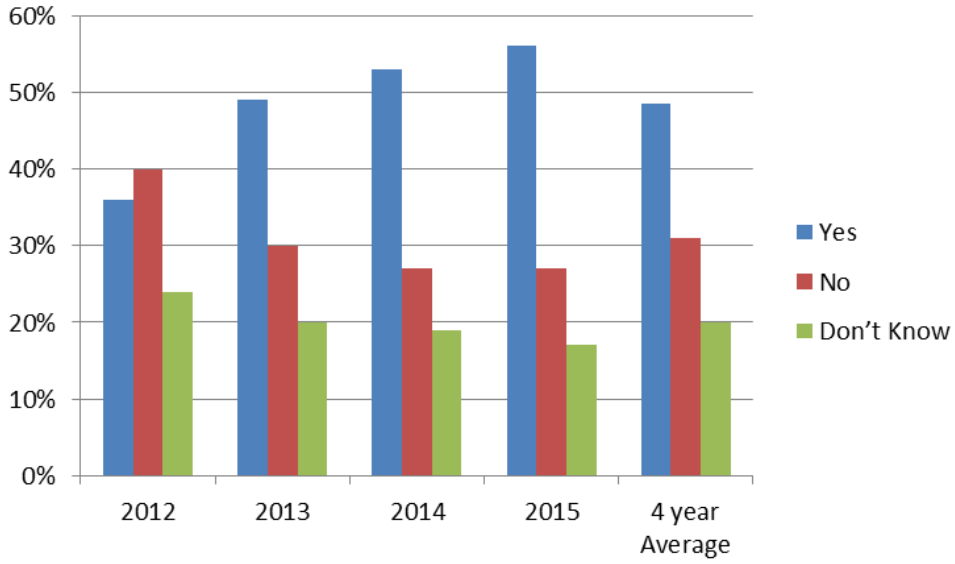
For a fourth year, respondents were asked, “Does your organization have a policy referred to as Bring Your Own Device (BYOD) policy?” Fifty-six percent responded yes, which is a 3 point increase from 2014 and 20 percentage points higher than in 2012 when the question was first asked.

exposure to loss. With this in mind, respondents were asked, “Does your organization have a mobile device security policy?” Seventy-nine percent of respondent said yes, an increase of 5 percentage points from the previous year. Larger organizations remain more likely to have a mobile device policy with 85 percent of large companies ($1 billion or greater) responding yes compared with 70 percent of smaller companies ($1 billion or less).

Additionally, organizations continue to increasingly focus on the security of non-company controlled mobile devices. For a fourth year, respondents were asked, “Does your organization have a policy referred to as Bring Your Own Device (BYOD) policy?” Fifty-six percent responded yes, which is a 3 point increase from 2014 and 20 percentage points higher than in 2012 when the question was first asked. (Exhibit 5)

EXHIBIT 5:

Does your organization have a Bring Your Own Device (BYOD) policy?



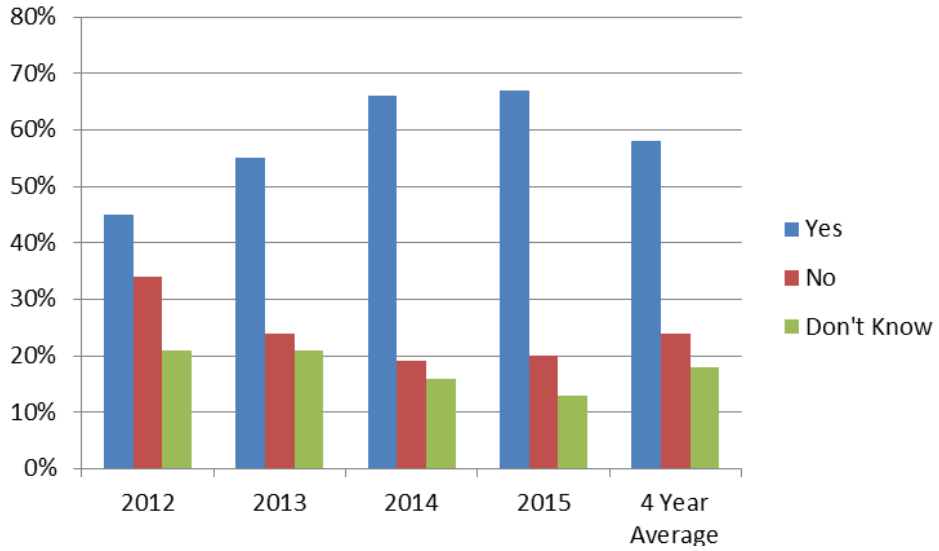
CLOUD SERVICES

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, is less than desirable for some organizations since control over the security of their data is handed over to the cloud services provider. Nonetheless, security concerns continue to be outweighed by the benefits. When asked, “Does your company use cloud services?” consistent with last year, 67 percent said yes. (Exhibit 6)

As a follow up, respondents were asked, “Is the assessment of vulnerabilities from cloud services part of your data security risk management program?” Fifty-six percent responded yes, up 4 percentage points from 2014.

EXHIBIT 6:

Does your company use cloud services?



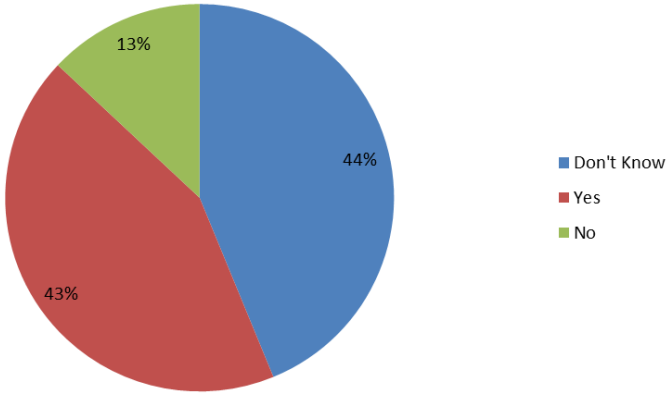
INTERNET OF THINGS (IOT)

A newer cybersecurity challenge for many organizations is the IoT, defined as everyday objects that have network connectivity, allowing them to send and receive data. Businesses increasingly look to smart technology to increase efficiency and overall competitiveness; this includes everything from fitness trackers to SCADA systems used in manufacturing. Respondents were asked, "Does your company have exposure to the IoT?" Forty-three percent said yes, 13 percent said no and the rest (44 percent) did not know. (Exhibit 7)

Businesses increasingly look to smart technology to increase efficiency and overall competitiveness; this includes everything from fitness trackers to SCADA systems used in manufacturing.

EXHIBIT 7:

Does your company have exposure to the IoT (Internet of Things)? (e.g., SCADA Systems &/or Internet connected devices other than a laptop etc.)



As a follow up, respondents were asked, “Are you proactively addressing bodily injury and property damage exposures as a result of IoT risks?” Twenty-nine percent said yes, 27 percent responded no, 9 percent indicated N/A and 35 percent did not know.

INFORMATION SECURITY AND CYBER RISK MANAGEMENT FOCUS

To better understand how organizations accomplish their information security and cyber risk management objectives, respondents were asked a series of questions on their cyber risk management efforts.

Greater awareness at the executive and board levels has led many organizations to hire a CIO or CISO to spearhead their information security risk management efforts. When asked, “Is there a key executive with oversight responsibility or whose main focus is cybersecurity?” 74 percent said yes. When looking at only the larger respondents (those with revenues in excess of $1 billion), the percentage jumps to 80 percent.

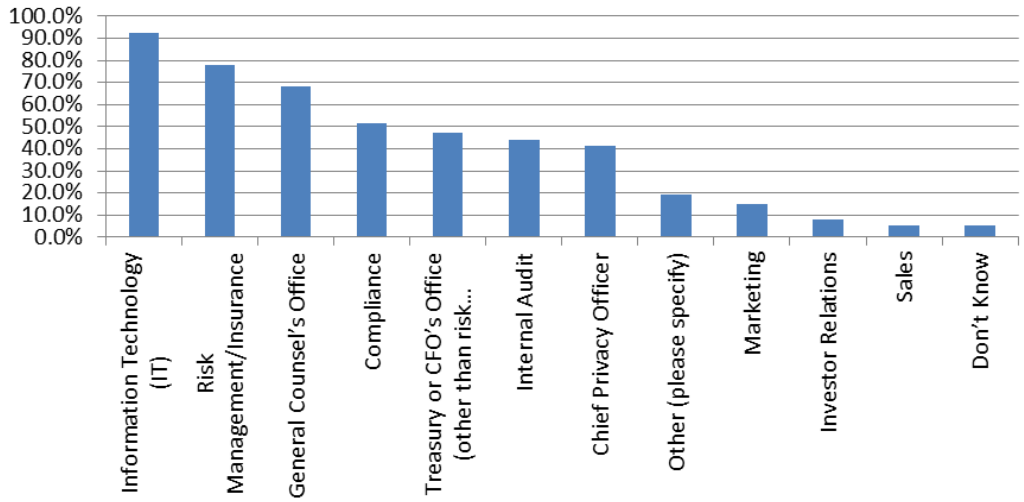
More organizations view information security as an organizational challenge rather than just an issue to be addressed by the IT department. Respondents were asked, “Does your organization have a multi-department information security risk management team or committee?” Fifty-seven percent said yes, an increase of five percentage points from last year and more in line with prior years. As in previous years, however, this varies materially based on the size of the company, with 65 percent of larger companies ($1 billion in revenue or greater) claiming to have this team or committee compared with 48 percent of smaller companies (under $1 billion in revenue).

GREATER AWARENESS AT THE EXECUTIVE AND BOARD LEVELS HAS LED MANY ORGANIZATIONS TO HIRE A CIO OR CISO TO SPEARHEAD THEIR INFORMATION SECURITY RISK MANAGEMENT EFFORTS.

Respondents were asked, “Which departments are represented on this team or committee?” Ninety-three percent said IT, 78 percent said Risk Management/Insurance, 68 percent said General Counsel, 52 percent said Compliance, 47 percent said Treasury or CFO’s Office, 44 percent said Internal Audit and 42 percent said Chief Privacy Officer. Common write-in responses under “Other” included Human Resources, Communications and Operations. (Exhibit 8)

EXHIBIT 8:

Which departments are represented on this team or committee?

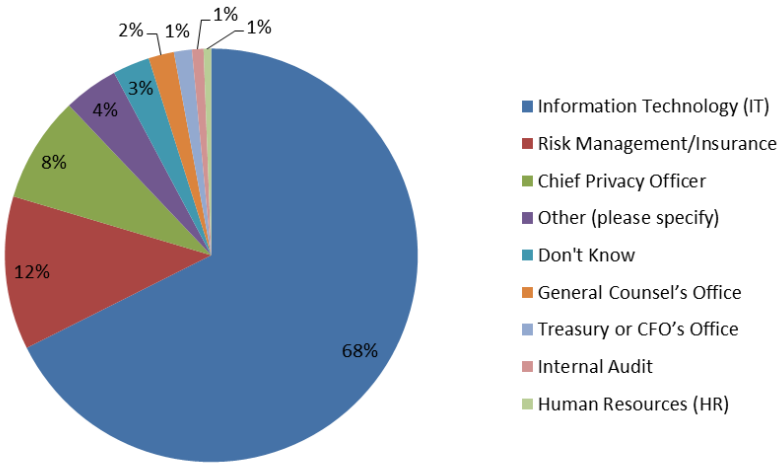


INFORMATION TECHNOLOGY (IT) IS NOT ONLY THE MOST REPRESENTED DEPARTMENT ON THE INFORMATION SECURITY RISK MANAGEMENT TEAM OR COMMITTEE; IT IS RESPONSIBLE FOR LEADING THE EFFORT IN MOST ORGANIZATIONS.

Information technology (IT) is not only the most represented department on the information security risk management team or committee; it is responsible for leading the effort in most organizations. In response to the question, "Which department is PRIMARILY responsible for spearheading the information security risk management effort?" 68 percent said IT. This is nearly identical with last year (69 percent) but significantly below the 2013 high (78 percent). Risk Management and Insurance came in a distant second at 12 percent (11 percent in 2014). (Exhibit 9)

EXHIBIT 9:

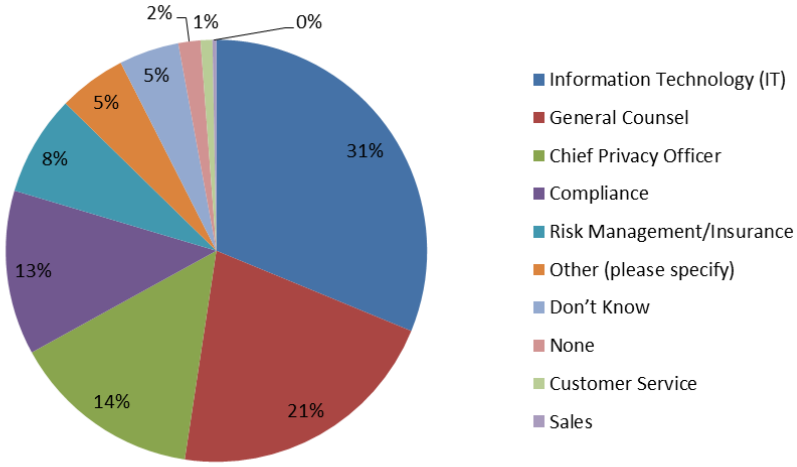
Which department is PRIMARILY responsible for spearheading the information security risk management effort?



Also consistent with previous years, IT remains the department most frequently responsible for assuring compliance with all applicable federal, state or local privacy laws including state breach notification laws. (Exhibit 10)

EXHIBIT 10:

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



Respondents were asked to describe how cyber risk awareness and cyber risk management has changed in their organization in the past three years. The biggest theme among respondents was that cyber risk has gained more visibility across all levels of the organization and more resources are being allocated toward preventing a cyber incident. Below are a few of the responses.

"We have become much more concerned about the risk of a cyber breach. We have updated policies and procedures and put new defenses in place. Additionally, we recently purchased cyber coverage, which we have not previously held."

"We have tightened internal security measures, isolated certain systems and integrated education and awareness of our employees with these changes. Additionally, we have secured a level of risk transfer that meets our objectives."

"There has been more vulnerability testing of systems and collaborations with other companies with our industry, including the U.S. government, concerning the methods of recent attacks/threats to help us stay current on how to best address cyber risk issues."

"It has moved from middle management to senior management. Human resources is great at what they do, but cyber is multi-faceted in dealing with crisis management, public relations, liability mitigation, management of insurance liability, dealing with stakeholders, etc. It has forced the C-suite to face not only cyber, but other critical insurance concerns such as D&O and business interruption."

The biggest theme among respondents was that cyber risk has gained more visibility across all levels of the organization and more resources are being allocated toward preventing a cyber incident.

THE ROLE OF INSURANCE

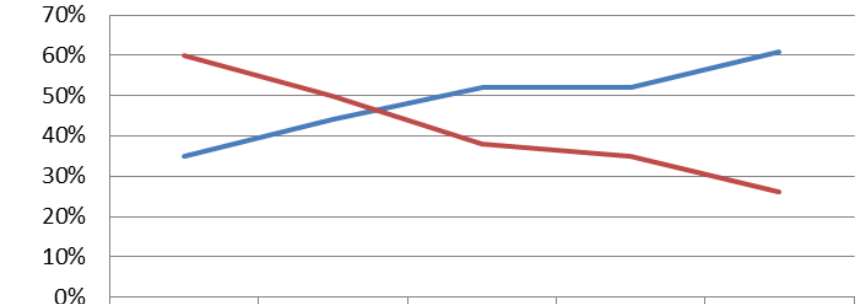
The plateau in the percentage of companies purchasing cyber liability insurance last year appears to have been only temporary as the overall upward trend accelerated in 2015. Participants were asked, "Does your organization purchase cyber liability insurance?" Sixty-one percent responded yes, 26 percent said no and 13 percent did not know. (Exhibit 11)

Overall, the percentage of respondents who purchase coverage has increased by 26 percentage points since 2011. The percentage of larger organizations (defined as having revenues greater than $1 billion) has increased 30 percentage points over that period (from 35 percent in 2011 to 65 percent in 2015), while the percentage of smaller organizations (defined as having revenues of $1 billion or less) has increased 22 percentage points.

OVERALL, THE PERCENTAGE OF RESPONDENTS WHO PURCHASE COVERAGE HAS INCREASED BY 26 PERCENTAGE POINTS SINCE 2011.

EXHIBIT 11:

Does your organization purchase cyber liability insurance?

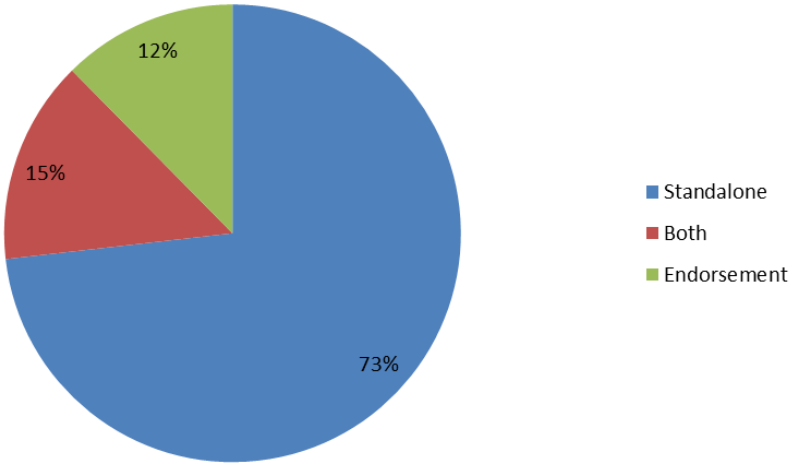


	2011	2012	2013	2014	2015
Yes	35%	44%	52%	52%	61%
No	60%	50%	38%	35%	26%

Of the respondents who purchase coverage, 73 percent purchase it on a standalone basis, 12 percent by endorsement and 14 percent purchase both. (Exhibit 12) This varies materially, however, by size of the company with 84 percent of larger organizations (greater than $1 billion in revenue) purchasing standalone coverage, compared with 62 percent of smaller organizations ($1 billion or less in revenues).

EXHIBIT 12:

Do you purchase cyber coverage on a standalone basis, by endorsement, or both?



Thirty-three percent of respondents have purchased the cover for less than two years, 34 percent between three and five years, and 33 percent for more than five years. For the first time, respondents were also asked if they have or are considering increasing the amount of coverage they purchase. Thirty percent said they have increased the amount of coverage, 36 percent said they are considering increasing the amount of coverage, and 34 percent said no to both.

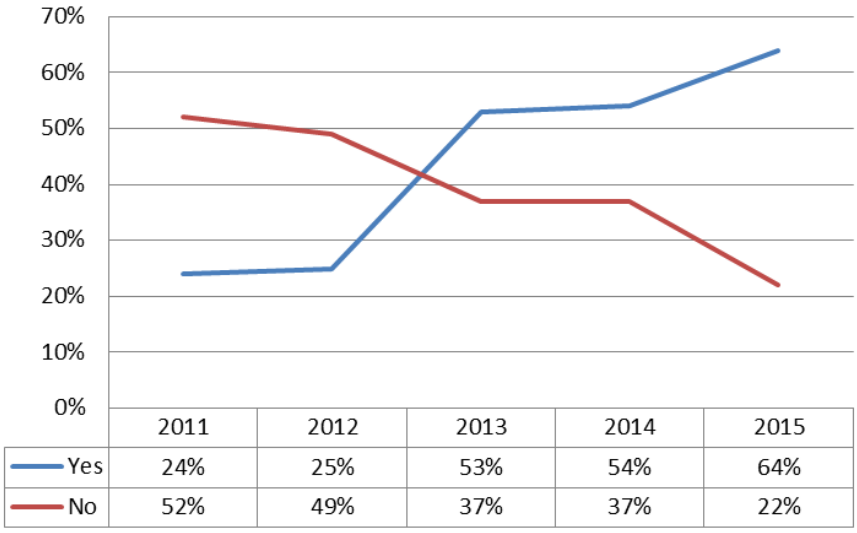
Of the respondents who have increased the amount of coverage, 44 percent have purchased coverage for more than 5 years, 31 percent between 3 and 5 years, and 16 percent less than two years. Of the respondents who are considering increasing the amount of coverage, 41 percent have purchased it for between 3 and 5 years, 33 percent for less than 2 years, and 32 percent for more than 5 years.

For the first time, respondents were also asked if they have or are considering increasing the amount of coverage they purchase. Thirty percent said they have increased the amount of coverage, 36 percent said they are considering increasing the amount of coverage, and 34 percent said no to both.

Respondents who do not currently purchase cyber insurance were asked, "What is the PRIMARY reason you have chosen not to purchase cyber liability insurance?" "My superiors do not see the need" is the most common response at 20 percent, followed by "lack of knowledge about the coverage" at 12 percent. Thirty-three percent responded "other," with the most common write-in answers being that they self-insure or are currently in the process of assessing options for purchase. When respondents were asked, "Are you considering buying this coverage in the next year?" 64 percent said yes, a 10 point increase from last year. (Exhibit 13)

EXHIBIT 13:

Are you considering buying this coverage in the next year?



	2011	2012	2013	2014	2015
Yes	24%	25%	53%	54%	64%
No	52%	49%	37%	37%	22%

CYBER RELATED BUSINESS INTERRUPTION/ CONTINGENT BUSINESS INTERRUPTION

When most risk professionals think about business interruption, lost income resulting from physical damage to property and equipment may be what first comes to mind. However, cyberattacks that damage critical data or render websites or technology infrastructure unusable should be of increasing concern. To gauge respondents' perception of this exposure, they were asked for the first time this year, "How concerned are you with cyber related business interruption (BI) & contingent business interruption (CBI) exposures?" Twenty-three percent are extremely concerned, 70 percent moderately concerned, 4 percent not at all concerned and 3 percent did not know.

To understand whether this concern was translating into an insurance purchase for the exposure, respondents who purchase cyber coverage were asked, "Do you currently buy coverage for your loss of income due to data breaches arising from your network?" Sixty-three percent said yes, 26 percent responded no and 11 percent did not know.

"How concerned are you with cyber related business interruption (BI) & contingent business interruption (CBI) exposures?" Twenty-three percent are extremely concerned, 70 percent moderately concerned, 4 percent not at all concerned and 3 percent did not know.

When comparing the level of concern and whether or not insurance was being purchased, 71 percent of respondents who said they are extremely concerned purchased cyber related business interruption coverage, and 61 percent who are moderately concerned purchase the cover.

ABOUT THE SURVEY RESPONDENTS

For a fifth consecutive year, Advisen and Zurich collaborated on a survey designed to gain insight into the current state and ongoing trends in information security and cyber liability risk management. Invitations to participate in the survey were distributed via email to risk managers, insurance buyers and other risk professionals. The survey was completed at least in part by 448 respondents.

The majority of respondents classified themselves as either Chief Risk Manager/Head of Risk Management Department (37 percent) or Member of Risk Management Department (not head) (35 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 25 percent with 11-20 years, 18 percent with 6 to 10 years and 13 percent with 5 years or less.

All 13 macro industry segments are represented. Healthcare has the highest representation accounting for 23 percent of the total respondents; followed by Professional Services at 17 percent; Industrials at 11 percent; Government and Nonprofit at 10 percent; Nonbank Financial at 8 percent; Consumer Discretionary at 6 percent; Education at 5 percent; Consumer Staples, Energy and Materials at 4 percent; Banks and Utilities at 3 percent; and Telecommunications at 2 percent.

The survey represents businesses from all sizes but is slightly weighted towards larger companies with 52 percent of respondent companies having revenues in excess of $1 billion. In terms of the number of employees, 26 percent of respondents have more than 15,000 employees, 25 percent have between 1001 and 5000, 23 percent have less than 500, 20 percent have between 5001 and 15,000, and 6 percent have between 500 and 1000.