Advisen
Transforming • Insurance℠

INFORMATION SECURITY AND CYBER RISK MANAGEMENT

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

Sponsored by

ZURICH®

October 2016

TABLE *of* CONTENTS

ZURICH® Advisen Transforming • Insurance™

EXECUTIVE SUMMARY

The cyber threat landscape continues to rapidly change and businesses of all sizes and across all industries are increasingly exposed. A recent announcement of a breach of 500 million records by a major multinational technology company, for example, serves as yet another unfortunate reminder that no business is immune to the threat of an information security incident.[1]

Sophisticated cybercriminals are defeating traditional approaches to cybersecurity, leaving organizations vulnerable to the costly and disruptive consequences of a data breach or other cybersecurity failure. Preparation and awareness at all levels of an organization are essential to helping reduce the likelihood of a breach and minimize its impact.

But how truly concerned are businesses? And how are they responding to these evolving threats?

With these questions in mind, Advisen and Zurich North America came together for a sixth consecutive year to study how business attitudes and strategies continue to evolve in information security and cyber risk management. The study represents a sustained commitment by both organizations to stay current with these evolving risks and the impact they have on businesses across the United States.

One theme that is constant throughout is a heightened need by businesses to become resilient against information security threats. As businesses work towards this resiliency goal, the insurance industry can play an important role in identifying emerging risks and responding to their needs.

KEY FINDINGS

- Eighty-seven percent of respondents believe a technology interruption would have a moderate-to-significant impact on their business. Still, 13 percent do not see technology interruption as even a moderate risk.
- Growth in the purchase of network security & privacy "cyber" insurance appears to be slowing, indicating the market is maturing. While the overall upward trend of organizations purchasing cyber insurance continued in 2016, it was up only seven percent from 2015.
- Over the last six years, the proportion of companies buying security & privacy cyber insurance has increased by 85%, from 35% in 2011 to 65% in 2016.
- For the first time in the six years of this study, general counsel has surpassed information technology (IT) as the department most frequently responsible for assuring compliance with all applicable federal, state or local privacy laws, including state breach notification laws.
- Most companies surveyed (97 percent) clearly recognize the importance of collaboration between their risk management and information technology (IT) departments on issues related to cyber security.
- Industries with substantial personally identifiable information (PII), personal health information (PHI) and/or personal financial information (PFI), in general, consider data security and privacy to be a more significant risk. As a result, they also are more likely to purchase security & privacy insurance and engage in risk management activities.
- Costs related to a breach of customer/personal information is the leading reason for purchasing "cyber" insurance.
- Majority of businesses are working to create a mindset of resilience by engaging in risk mitigation assessment and response plans.

[1] Mike Snider and Elizabeth Weise, USA Today, "500 million Yahoo accounts breached," (September 22, 2016), http://www.usatoday.com/story/tech/2016/09/22/report-yahoo-may-confirm-massive-data-breach/90824934/

"But the level of cyber risk concern is subject to a variety of factors and brings to light two different profiles within the business community: industries that collect substantial personal data (such as healthcare, communications, financial and banking, and retail) and those that do not."

ANALYSIS AND CONCLUSIONS

A lot has changed in information security and cyber risk management since 2011, the first year of this study. Hardly a week has passed without a report of high-profile data breach and just about every sector of the U.S. economy has been a target.

Over the past six years, this study has documented a marked shift in the attitude of risk professionals, executives and board members around cyber risk. Data breaches were once considered an unlikely event but are now expected to occur.

These changing views of risk professionals, executives, and boards are evident through a shifting approach to information security and cyber risk management. In the past, cyber risk was often considered as exclusively an IT issue. Now, it increasingly receives a multi-departmental risk management focus that requires participation from the mailroom to the boardroom, as well as input from external resources.

But the level of cyber risk concern is subject to a variety of factors and brings to light two different profiles within the business community: industries that collect substantial personal data (such as healthcare, communications, financial and banking, and retail) and those that do not.

These personal data-driven industries often have a higher degree of regulatory oversight and are further along in their understanding of cyber-related risk. The results of this study show that, in general, these industries view cyber risk more seriously, have more robust cybersecurity and risk management strategies, and are more likely to purchase a security and privacy insurance policy.

For example, 37 percent of the survey's respondents come from personal data-driven industries, of which 76 percent view cyber risk as a significant threat. In comparison, of the 63 percent of respondents from all other industries, only 55 percent view cyber risk as a serious threat.

Likewise, 78 percent of respondents from personal data-driven industries purchase a security & privacy insurance policy, compared with only 59 percent from all other industries.

Over the six years of this study, the cyber risk awareness of businesses outside the personal data-driven industries has grown, but there are still some who believe their exposure is minimal. For example, the top reason respondents do not purchase a security & privacy insurance policy is they believe their organization is not susceptible to a cyber-related loss.

But these businesses are in the minority. As the level of awareness and concern grows, many businesses outside of personal data-driven enterprises believe they are exposed to a cyber-related loss. They want to become more resilient and take steps to ensure their organizations are able to prevent, detect, respond to and recover from information security incidents as quickly as possible. Preparedness is a key aspect to this resiliency and, according to the study, most have implemented at least some pre-breach risk management activities, many provided through internal resources.

The personal data-driven industries, however, are more likely to look for assistance outside the organization, particularly for pre-breach services. For example, overall the pre-breach service most commonly provided by external resources is a cyber risk management program assessment. Fifty-five percent of respondents from the personal data-driven segments look externally for this service, compared with 42 percent from all other industries. Most of the other pre-breach services, such as assessing procedures for protecting sensitive data, evaluating the company's ability to detect and respond to indicators of data compromise, and employee training have similar findings.

Also, since cyber risk is more frequently viewed as an enterprise-wide issue, departments such as general counsel and risk management are now taking on larger roles. The study revealed that approximately 60 percent of pre-breach services are provided by internal resources such as IT, risk management, human resources (HR) and legal.

In recent years, cybercriminals have focused on the "human element" through social engineering tactics, such as phishing and spear phishing email. The survey respondents appear to recognize this threat, indicating the issue of greatest concern is employees unintentionally infecting the network with malware.

"THERE REMAINS A GREAT NEED FOR GUIDANCE IN DEVELOPING INFORMATION SECURITY AND CYBER RISK MANAGEMENT PROGRAMS AND IMPROVING CYBER RISK RESILIENCY."

Managing risk from inside the organization through employee education is vital to help prevent and respond to social engineering campaigns. But according to the study, about 21 percent of respondents report they still do not have an employee education program.

Taken as a whole, there remains a great need for guidance in developing information security and cyber risk management programs and improving cyber risk resiliency. This is an opportunity for the insurance industry to bring value by helping to develop strategic cyber prevention and response initiatives, and demonstrating the benefits of security & privacy insurance policies.

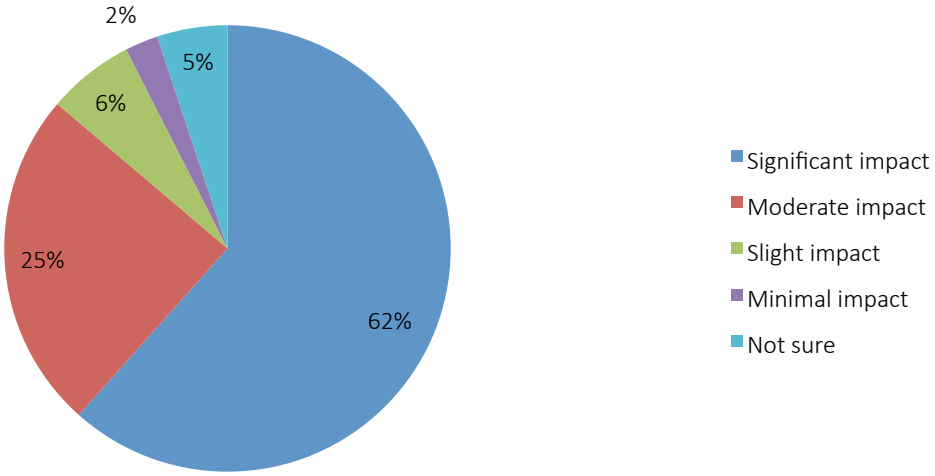
PERCEPTION OF CYBER RISK

RISK PROFESSIONALS

Risk professionals continue to view cyber as a serious threat. When asked to what extent an internet, cloud or technology disruption would impact their daily business operations, 87 percent said it would have a moderate-to-significant impact (see Exhibit 1).

EXHIBIT 1:

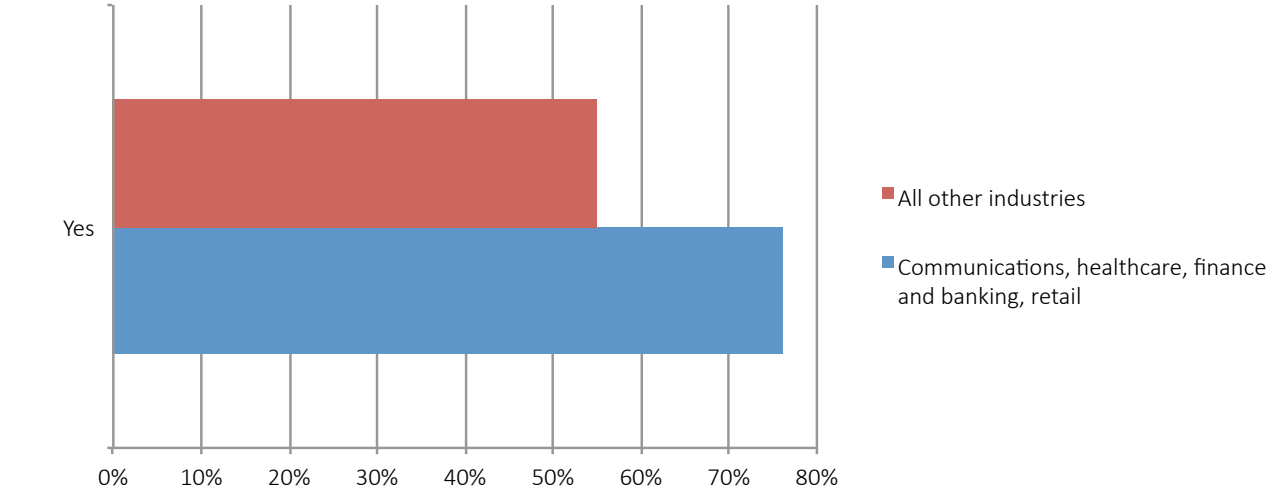
To what extent would an internet, cloud or technology disruption impact your daily business operations?



Industry, however, can influence this perception. Industries with substantial PII, PHI and/or PFI consider cyber risk in general to be a more significant threat. For example, 76 percent of respondents in the communications, healthcare, finance and banking, and retail industries viewed cyber risk as a significant threat compared to only 55 percent of all the other industries (see Exhibit 2).

EXHIBIT 2:

Would an internet, cloud or technology disruption have a significant impact on your daily business operations?



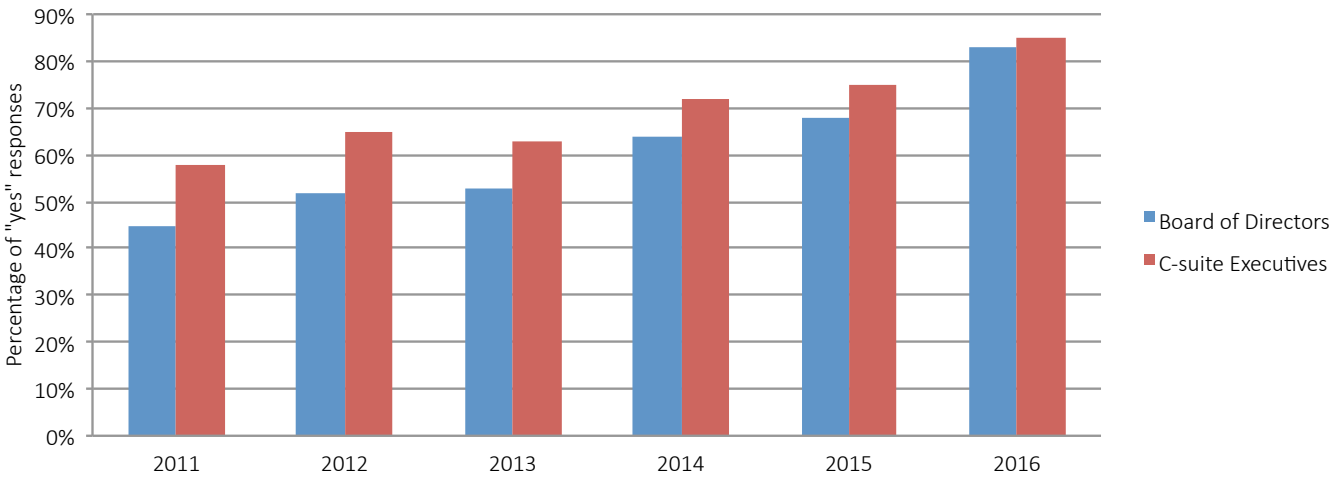
BOARDS AND EXECUTIVE MANAGEMENT

Boards and executive management also continue to view cyber risks more seriously and the gap in risk perception between the two continues to close. In response to the question, "In your experience, are cyber risks viewed as a significant threat by your organization's leadership?" 83 percent said "yes" for Board of Directors. That is a substantial 15 percentage points higher than in 2015 and 38 percentage points higher than the first survey in 2011.

Eighty-five percent said "yes" for C-suite executives, 10 percentage points higher than 2015 and 27 points higher than the first survey in 2011 (see Exhibit 3).

EXHIBIT 3:

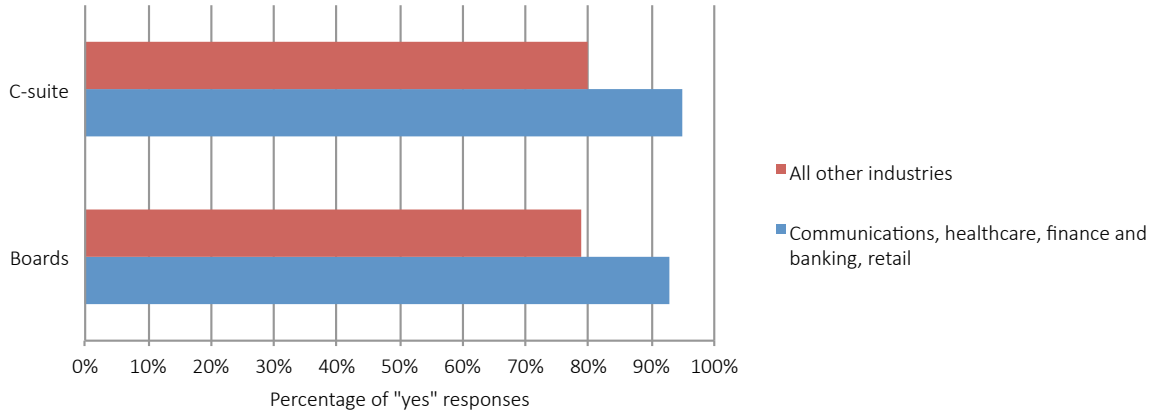
In your experience, are cyber risks viewed as a significant threat by your organization's leadership?



Industry also influences the cyber risk perception of boards and executive management. When again looking at the communications, finance and banking, healthcare, and retail industries, 93 percent of boards and 95 percent of C-suite executives view cyber risk as a significant threat. Conversely, 79 percent of boards and 80 percent of C-suite executives from all the other industries view cyber risk as a significant threat (see Exhibit 4).

EXHIBIT 4:

Are cyber risks viewed as a significant threat? (PII-, PHI- and PFI-driven segments vs. all other industries)

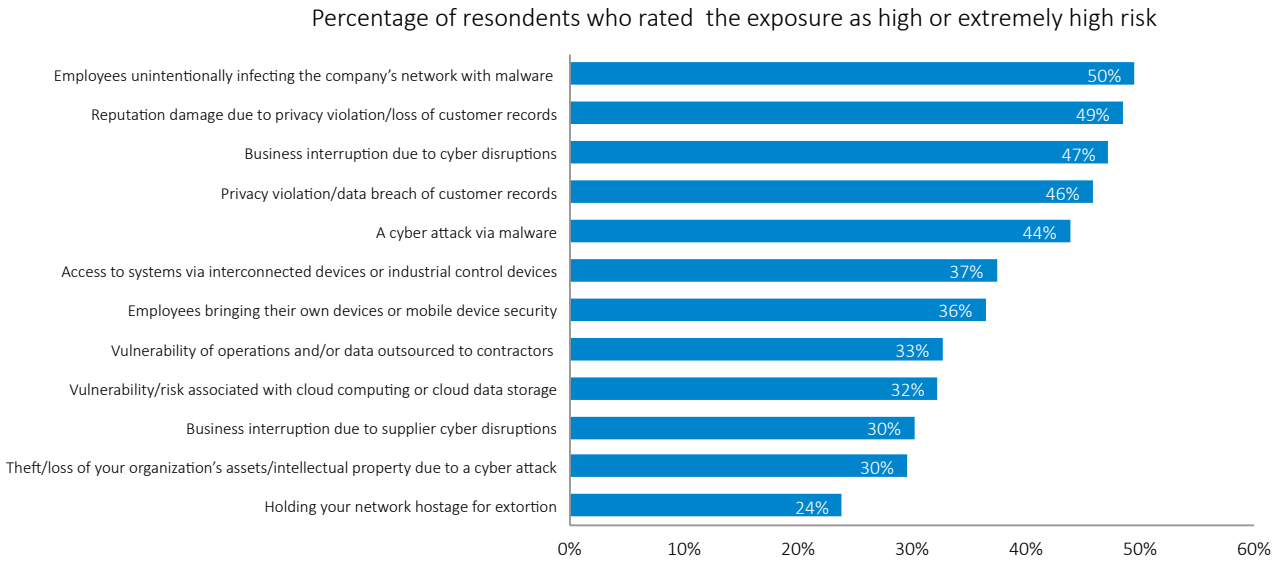


EXPOSURES

Respondents were asked to rate 12 cyber exposures on a five-point scale, ranging from extremely low risk to extremely high risk. According to all respondents, "employees unintentionally infecting the company's network with malware" is the top concern with 50 percent rating it a high or extremely high risk. "Reputation damage due to privacy violation/loss of customer records" came in a close second, with 49 percent rating it a high or extremely high risk and "business interruption due to cyber disruptions" rounded out the top three with 47 percent (see Exhibit 5).

EXHIBIT 5:

From the perspective of your organization, please rate each of the following risks.



"Industry again has a significant influence on this perspective. Respondents from the four industries identified as having substantial PII, PHI, and/or PFI (communications, healthcare, finance and banking, retail) said "reputation damage due to privacy violation/loss of customer records" is their top concern..."

Industry again has a significant influence on this perspective. Respondents from the four industries identified as having substantial PII, PHI, and/or PFI (communications, healthcare, finance and banking, retail) said "reputation damage due to privacy violation/loss of customer records" is their top concern, with 69 percent rating it a high or extremely high concern. This is compared to 38 percent rating it a high or extremely high concern from all the other industries.

Other top concerns of these personal data driven segments include "privacy violation/data breach of customer records" at 68 percent and "business interruption due to cyber disruptions" at 64 percent.

CYBER RISK MANAGEMENT: PREPARATION AND RESPONSE

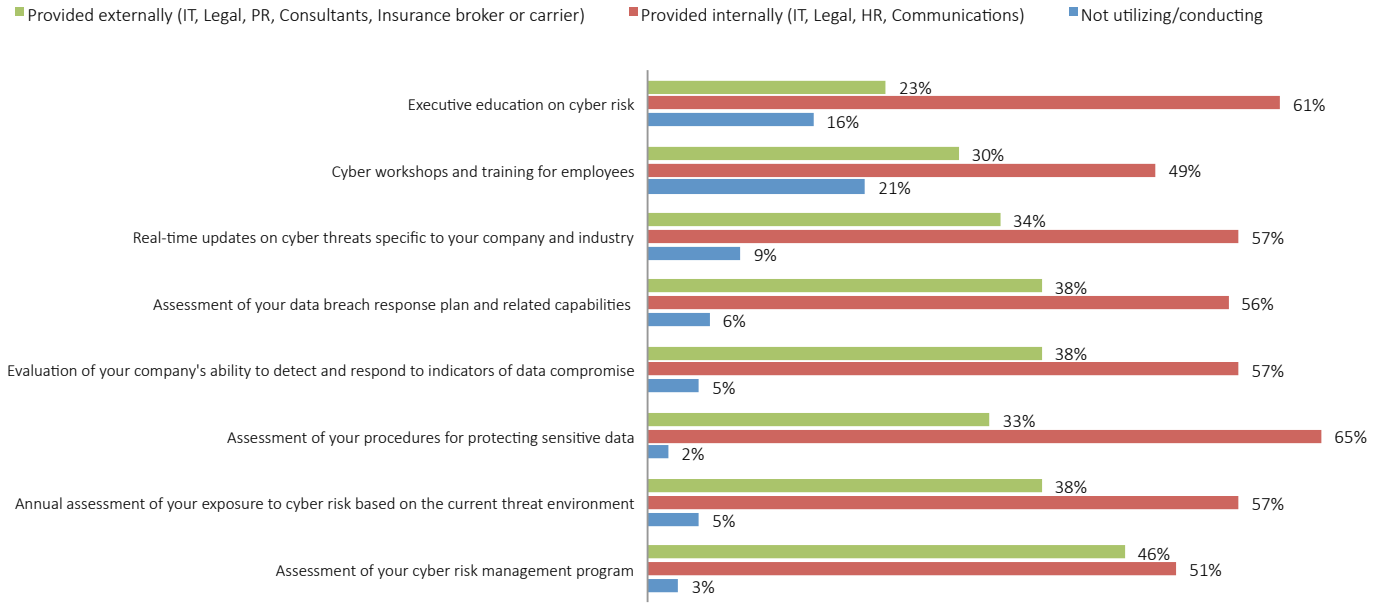
The consequence of an information security incident can be severe. From the cost associated with responding to the event, to an interruption of business operations, to a tarnished reputation, it can impact both the short- and long-term health of the business.

With more risk professionals and senior leaders viewing cyber risk as a significant threat, a greater focus has been put on preparation. When a breach occurs, a number of things must happen quickly and in a coordinated fashion or it can rapidly become a crisis that spirals out of control. Companies that are prepared and take an enterprise approach to cyber risk management can be in a much better position to effectively respond when a breach is discovered.

With this in mind, respondents were asked what kind of pre-breach services they utilized and how they were provided. Assessing procedures for protecting sensitive data is the service most commonly provided by internal resources; evaluating the company's ability to detect and respond to indicators of data compromise is the service most commonly provided by external resources; and assessment of cyber risk management programs is the service most commonly provided by insurance industry carriers and brokers (see Exhibit 6).

EXHIBIT 6:

What kind of pre-breach services does your company use and who provides these services?

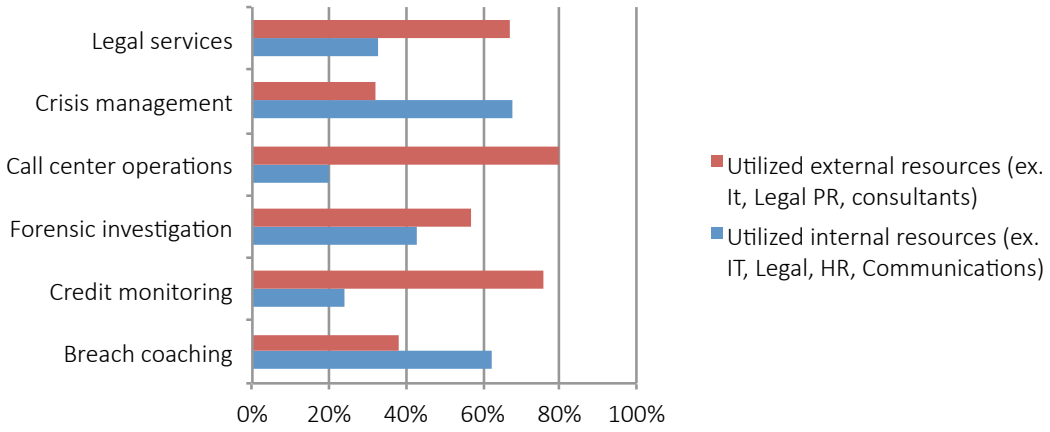


Developing a robust response capability well in advance of a breach can decrease the pressure on the business, lowers costs and reduces errors. This capability requires a high level of expertise. The study revealed that many businesses still primarily manage pre-breach planning, such as providing education for executives on cyber risk and assessing procedures for protecting sensitive data, from the inside the company. To do this effectively requires substantial resources typically only available to the largest organizations. As a result, the likelihood is high that many are not adequately prepared for a smooth and effective response.

External resources, however, are relied upon more frequently than internal resources in post-breach situations. Respondents who had experienced a breach resulting in economic loss were asked which, if any, services they engaged to respond to the breach. Crisis management is the post-breach service where internal resources are most commonly utilized (68 percent) and call center operations (80 percent) is the service where external resource are most commonly utilized (see Exhibit 7).

EXHIBIT 7:

Please indicate which, if any, services you engaged to respond to the breach.



A smooth breach response also requires compliance with all applicable federal, state or local privacy laws. Cybersecurity had long been viewed as a function of IT, so it was not surprising that in previous years IT was the department most frequently responsible for maintaining compliance. But as cyber risk has increasingly become an executive- and board-level concern, as well as an enterprise-wide focus, this is changing.

For the first time, general counsel is the department most frequently responsible for assuring compliance with all applicable federal, state or local privacy laws, including state breach notification laws (see Exhibit 8). Additionally, 55 percent of risk management teams regularly work with their colleagues in IT on cyber security issues (see Exhibit 9). The importance of compliance is represented in the increased role of general counsel and demonstrates the influence of regulation and heightened awareness of the legal issues that result from a data breach.

"FOR THE FIRST TIME, GENERAL COUNSEL IS THE DEPARTMENT MOST FREQUENTLY RESPONSIBLE FOR ASSURING COMPLIANCE WITH ALL APPLICABLE FEDERAL, STATE OR LOCAL PRIVACY LAWS, INCLUDING STATE BREACH NOTIFICATION LAWS..."

EXHIBIT 8:

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 breach notification laws?

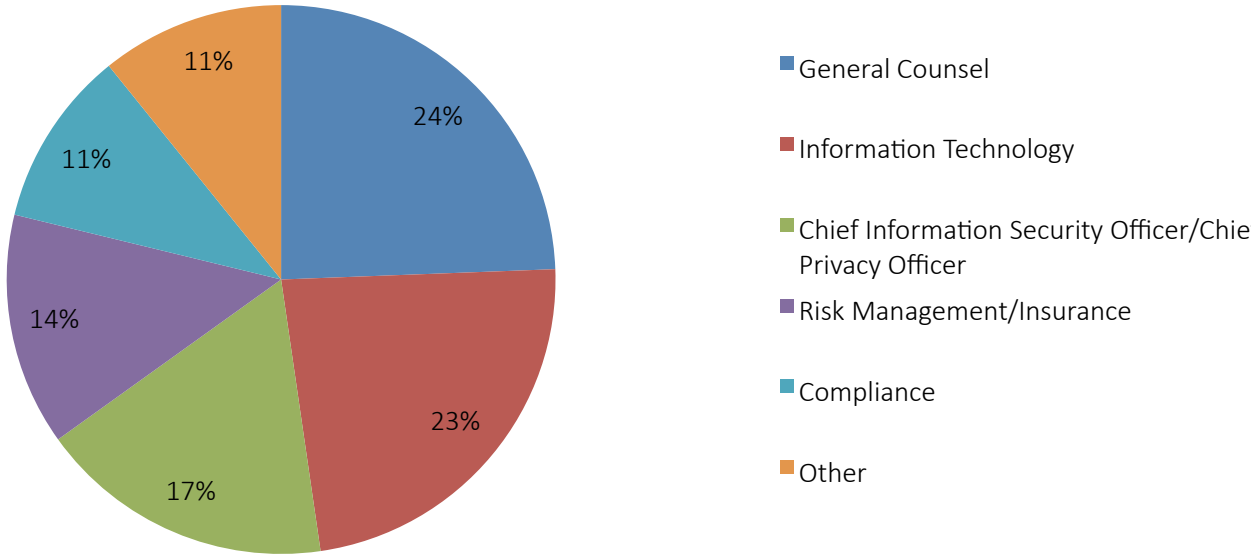
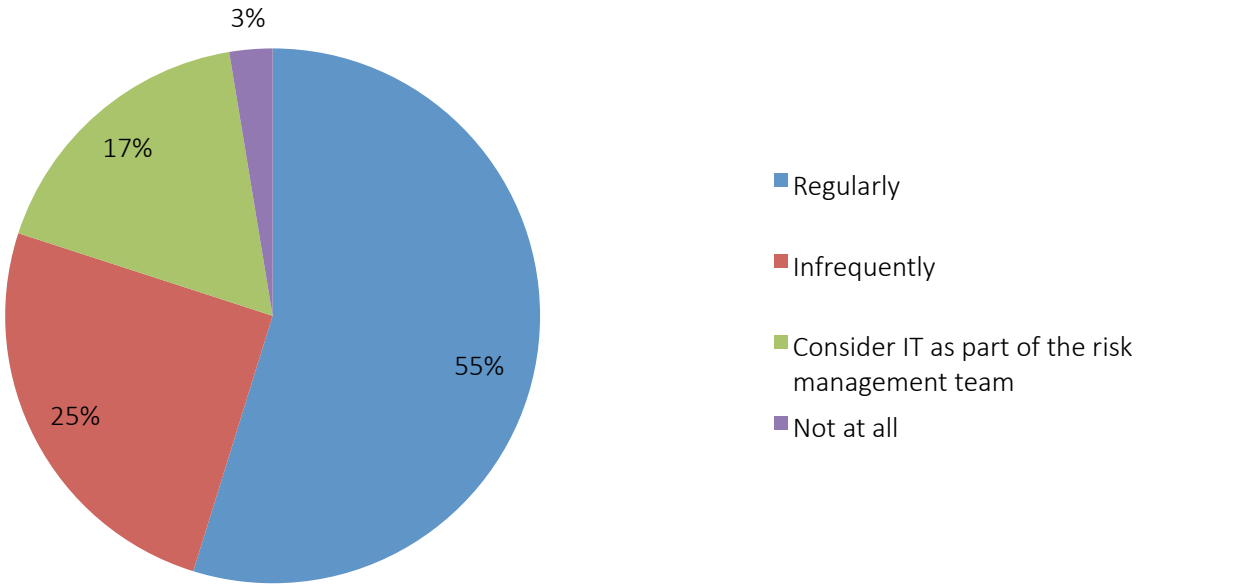


EXHIBIT 9:

In your organization, how closely do members of the risk management team work with their colleagues in IT?



SECURITY & PRIVACY INSURANCE

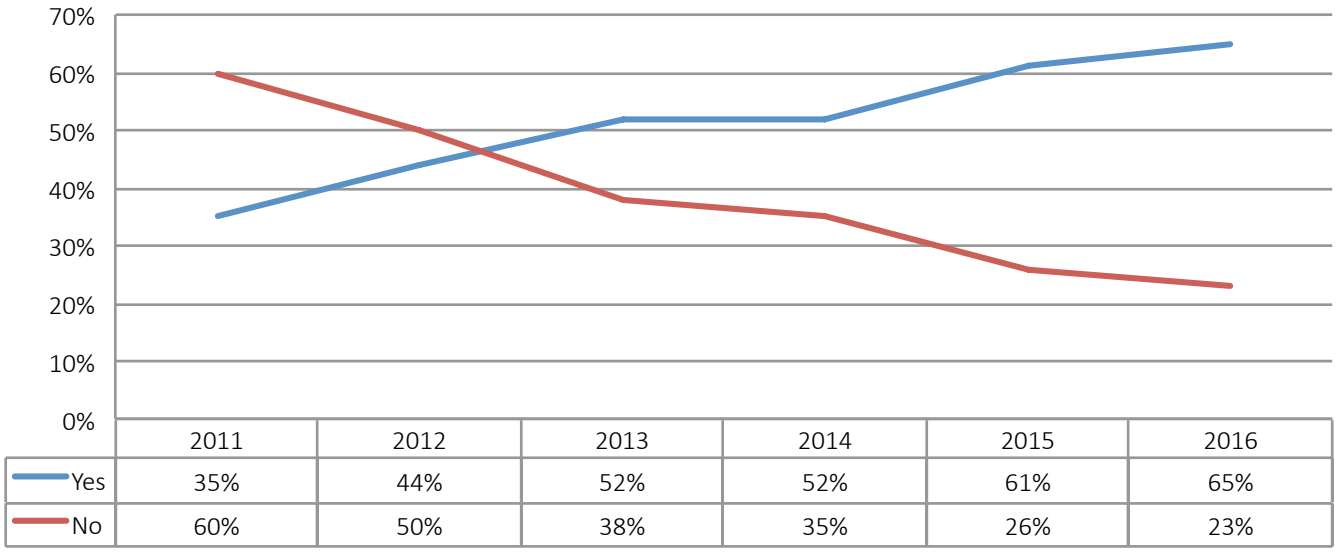
Security & privacy insurance continues to play a growing role in corporate cyber risk management programs. Participants were asked, "Has your company purchased security & privacy insurance?" Sixty-six percent responded "yes," 23 percent said "no," and 11 percent said they did not know (see Exhibit 10).

When looking only at the industries identified as having significant personal data exposures (communications, healthcare, financial and retail), 78 percent purchased security & privacy insurance compared with 59 percent from all other industries.

Overall, the percentage of respondents who purchase security & privacy insurance has increased by 31 percentage points since 2011. The percentage of large companies (defined as having revenues in excess of $1 billion) has increased 35 percentage points over that period (from 35 percent in 2011 to 65 percent in 2015), while the percentage of small companies (defined as having revenues of $1 billion or less) has increased 26 percentage points.

EXHIBIT 10:

Has your company purchased security & privacy insurance?



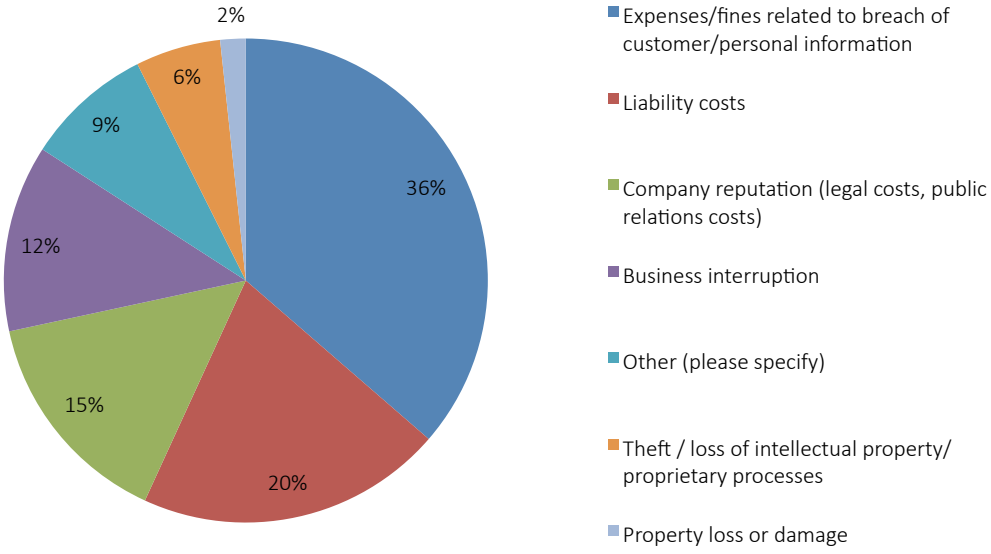
	2011	2012	2013	2014	2015	2016
Yes	35%	44%	52%	52%	61%	65%
No	60%	50%	38%	35%	26%	23%

"WHEN LOOKING ONLY AT THE INDUSTRIES IDENTIFIED AS HAVING SIGNIFICANT PERSONAL DATA EXPOSURES (COMMUNICATIONS, HEALTHCARE, FINANCIAL AND RETAIL), 78 PERCENT PURCHASED SECURITY & PRIVACY INSURANCE COMPARED WITH 59 PERCENT FROM ALL OTHER INDUSTRIES."

Of the respondents who purchase security & privacy insurance, the primary driver behind the insurance purchasing decision is expenses/fines related to a breach of customer/personal information at 36 percent. This was followed by liability costs at 20 percent. Interestingly, business interruption was the primary driver of the insurance purchasing decision of just 12 percent of respondents, yet it was rated a top three risk overall (see Exhibit 11).

EXHIBIT 11:

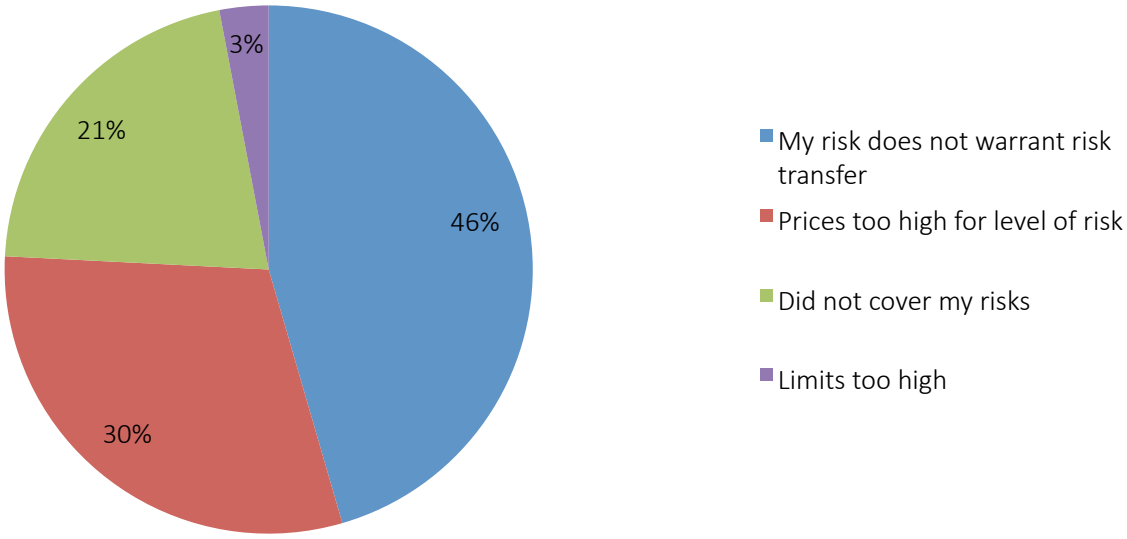
What was the primary reason for purchasing security and privacy insurance?



Continued growth in the "cyber" insurance market seems likely since 60 percent of respondents who do not currently purchase the coverage have considered purchasing it at some point. While 45 percent of respondents do not purchase security & privacy insurance because they think their risk does not warrant risk transfer, the remaining 55 percent currently do not because of market and product limitations. These are limitations that very well could change in the future (see Exhibit 12).

EXHIBIT 12:

Why did your company choose not to purchase security and privacy insurance?



ABOUT THE SURVEY RESPONDENTS

For a sixth consecutive year, Advisen and Zurich North America collaborated on a survey designed to gain insight into the current state and ongoing trends in information security and cyber 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 345 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 (37 percent).

Many industries are represented. Healthcare has the highest representation at 16 percent of the total; followed by finance, banking and insurance at 12 percent; manufacturing at 11 percent; other at nine percent; public administration, education, energy and mining, and technology all at six percent; education and technology both at six percent; services at five percent; retail trade, real estate and construction all at four percent; government and transportation both at three percent; hospitality at two percent; automotive and communications both at one percent; and wholesale trade at 0.3 percent.

Businesses of all sizes responded to the survey. Overall, the survey is slightly weighted towards smaller companies, with 53 percent of respondent companies having revenues of $1 billion or less. In terms of number of employees, 24 percent of respondent companies have between 1,001 and 5,000, 22 percent have more than 15,000, 18 percent have between 5,001 and 15,000, another 18 percent have less than 250, 10 percent have between 501 and 1000, and seven percent have between 251 and 500.

More information on cyber-related risks and solutions is available at http://www.zurichna.com/cyber.