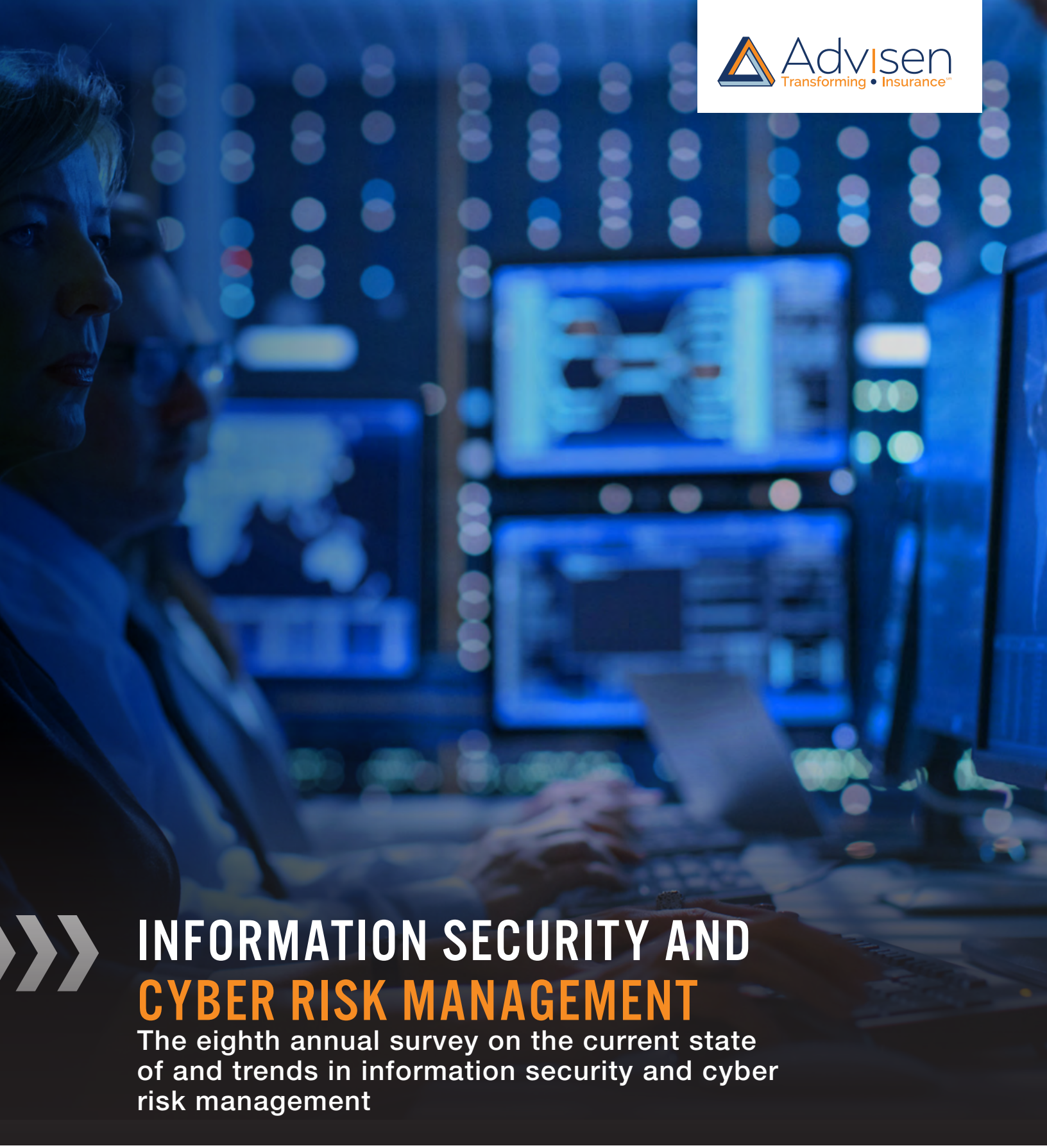


Advisen
Transforming • Insurance™

# INFORMATION SECURITY AND CYBER RISK MANAGEMENT

The eighth annual survey on the current state of and trends in information security and cyber risk management

OCTOBER

2018

*Sponsored by*

ZURICH®

> The nature of cybersecurity is evolving so quickly it can be difficult for businesses to keep track of the risks, let alone the solutions.
>
> Cyber is top of mind for businesses all across North America.
>
> At Zurich, we continue to invest in the cybersecurity arena and continue to work to identify risks and deliver solutions for businesses. That is why we have worked with Advisen for eight consecutive years to develop and execute this survey. The results provide a critical snapshot of the attitudes, concerns and actions of risk managers working to protect their businesses from cyber-related risks. It is our responsibility to respond to those needs and concerns with innovative services and solutions.
>
> —Paul Horgan, Head of North America Commercial Insurance for Zurich North America

# INFORMATION SECURITY AND CYBER RISK MANAGEMENT

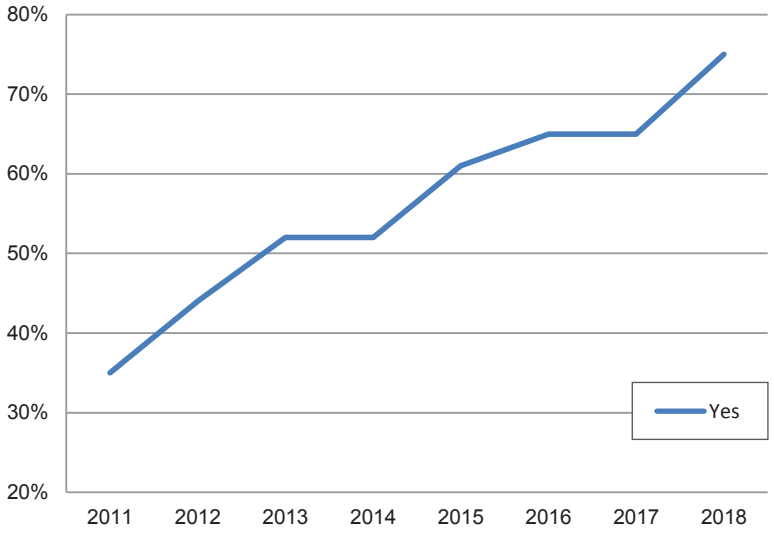
*The eighth annual survey on the current state of and trends in information security and cyber risk management*

## Executive Summary

The eighth annual Information Security and Cyber Risk Management survey from Zurich North America and Advisen Ltd. includes responses from risk professionals to gain a deeper understanding of corporate attitudes and strategies around cyber risk. Consistent with previous years, the 2018 study was designed to provide a benchmark for cyber risk strategies and to identify areas where insurance can bring value through strategic cyber prevention and response initiatives.

A key trend throughout the eight years of this study has been a growing reliance on insurance. The percentage of companies who purchase cyber insurance, either via stand-alone policies or endorsements, has increased 40 percentage points since 2011. The results of this year's study show a 10 percentage point uptick from 2017, the largest year-over-year increase since the first survey.

### DOES YOUR COMPANY CURRENTLY PURCHASE CYBERSECURITY INSURANCE?




2018 saw several high-profile cyber events — data security losses impacting millions of consumer's personal identifiable information and attacks that swept through businesses, shutting down operating systems and in many cases slowing or actually halting business operations. The growing reliance on cyber insurance indicated in the survey is, at least in part, a result of two factors: recent regulatory changes and a growing concern about business continuity losses.

The results revealed, however, a divergence between the purchasing preferences and experiences of large (i.e., revenue of more than $1 billion) versus middle market (i.e., revenue of less than $1 billion) companies.

## HIGHLIGHTS

### Regulatory changes had different influences on the cybersecurity approaches of large and middle market companies.

On May 25, the European Union's (EU) General Data Protection Regulation (GDPR) became law, increasing the financial and operational stakes for any organization handling the personal information of EU residents. Although compliance with the regulation can be onerous, the cost of compliance is significantly less than the potential penalties for violations, which can be as high as 20 million euros or four percent of an organization's global annual revenue.

The regulation applies to all companies regardless of size, industry, or location as long as they handle consumer data of EU residents. The survey revealed that large organizations are more concerned about the risk of non-compliance than middle market companies, and are therefore more likely to make changes to their cybersecurity controls as a direct result of the regulation.

According to the study:

- Nearly twice as many large companies made changes to their cybersecurity controls as a result of GDPR compared with middle market companies.
- Many companies with less than $1 billion in revenue believe that GDPR does not impact their organization because they do not collect consumer data or have operations in the EU.
- When asked the primary reason for purchasing cyber insurance, seven times as many large companies as middle market companies cited regulatory interpretation or uncertainty (GDPR/payment card industry [PCI]/Health Insurance Portability and Accountability Act [HIPAA]).

## Business continuity events grabbed headlines in 2017, but responses to these events from a risk mitigation and risk transfer standpoint differed by company size.

Business continuity risks are threats that disrupt the normal functions of a company's personnel and assets. These exposures were brought to the forefront in 2017 in large part due to a handful of cyberattacks such as the Dyn distributed denial of service (DDoS) attack, WannaCry and NotPetya, which caused significant losses to businesses around the world. While these business continuity events were certainly a wake-up call for all businesses, the survey revealed large companies viewed them as a greater concern from risk mitigation and risk transfer standpoints.

According to the study:

- Large companies expressed a higher degree of concern about business continuity risks than their middle market counterparts.
- Although middle market companies expressed less concern over business continuity risks, they have been more frequently impacted by business interruption losses.
- Large companies were more likely than middle market companies to mitigate supply chain risk using a variety of tools available to them.

## Sophistication regarding risk mitigation and risk transfer continues to vary by company size.

While the goal of Chief Information Security Officers and IT department heads is to prevent cyber incidents from occurring, the reality is even the most secure organizations have vulnerabilities. When a cyber incident occurs, a coordinated and well-rehearsed response has proven to significantly reduce the impact.

Many organizations are taking a multifaceted approach to their preparation and response strategies. This can be a complicated process, but it can make all the difference when trying to keep a data breach or other cyber event from spiraling out of control.

Many organizations are taking a multifaceted approach to their preparation and response strategies. This can be a complicated process, but it can make all the difference when trying to keep a data breach or other cyber event from spiraling out of control.

According to the study:

- Twice as many middle market companies as large companies said cyber supply chain risks had not affected their vendor management controls.
- Large companies were 20 percent more likely than their middle market counterparts to have altered their cybersecurity program in the past year due to the evolving threat landscape.
- Through 2015, large companies were more likely than middle market companies to purchase cybersecurity insurance. However, over the last three years a higher percentage of middle market companies than large companies have purchased the coverage for the first time.

# KEY FINDINGS

## Regulatory changes influenced large and middle market companies differently.

Several cyber-related issues have jumped to the forefront in 2018. One was the implementation of the EU's GDPR and the requirements it places on businesses handling personal information of EU residents.

With this in mind, respondents were asked if their organizations made changes to cybersecurity controls as a result of GDPR. Interestingly, only 40 percent of respondents said that they had made changes.

The size of the company, however, was a significant variable as to whether GDPR influenced their cybersecurity controls. It was noted that 49 percent of large companies made changes to their cybersecurity controls as a result of GDPR, compared with just 28 percent of middle market companies.

Respondents were asked to explain some of the changes they made, if any.

One respondent from a large organization said, "A third party was engaged to assist us in evaluating our security/safeguarding of data, system security and our controls and protocols. Recommendations were evaluated and changes implemented as deemed appropriate. We have also established a four-part IT/security training course mandatory for all non-manufacturing employees."

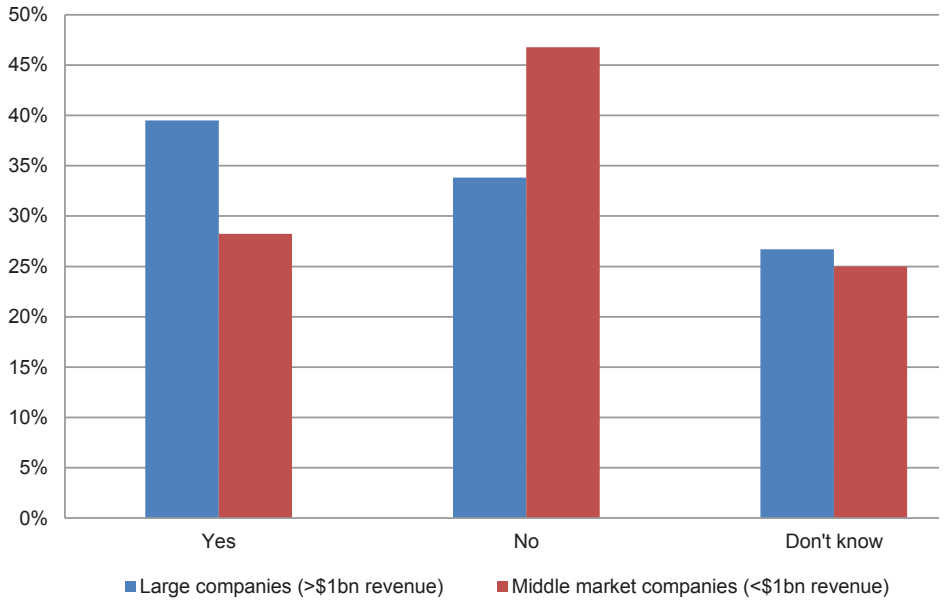
Another respondent from a large organization said, "Our interactive internet platform has a comprehensive GDPR-compliant policy and an introductory page (that links to the comprehensive policy) that highlight salient points and requires acceptance that is retained with the login ID info."

A common theme throughout the responses of middle market companies was that GDPR does not impact their organization because they do not collect consumer data or they do not have operations in the EU. Advisen research suggests that many mid-size U.S. companies have GDPR exposure, but are unaware of it (e.g., they have customers who are EU citizens, but reside in the U.S). This implies that many U.S. companies lack an understanding of the regulation and of the controls needed for compliance. It also illustrates an opportunity for insurance professionals to provide guidance on the regulation and the cybersecurity controls necessary to maintain appropriate security.

"While we believe that our policies and controls were already compliant with GDPR, we do no international business, nor do we engage in business with international clients. All of our clients, both at present and in the foreseeable future, are U.S. companies," said one middle market respondent.

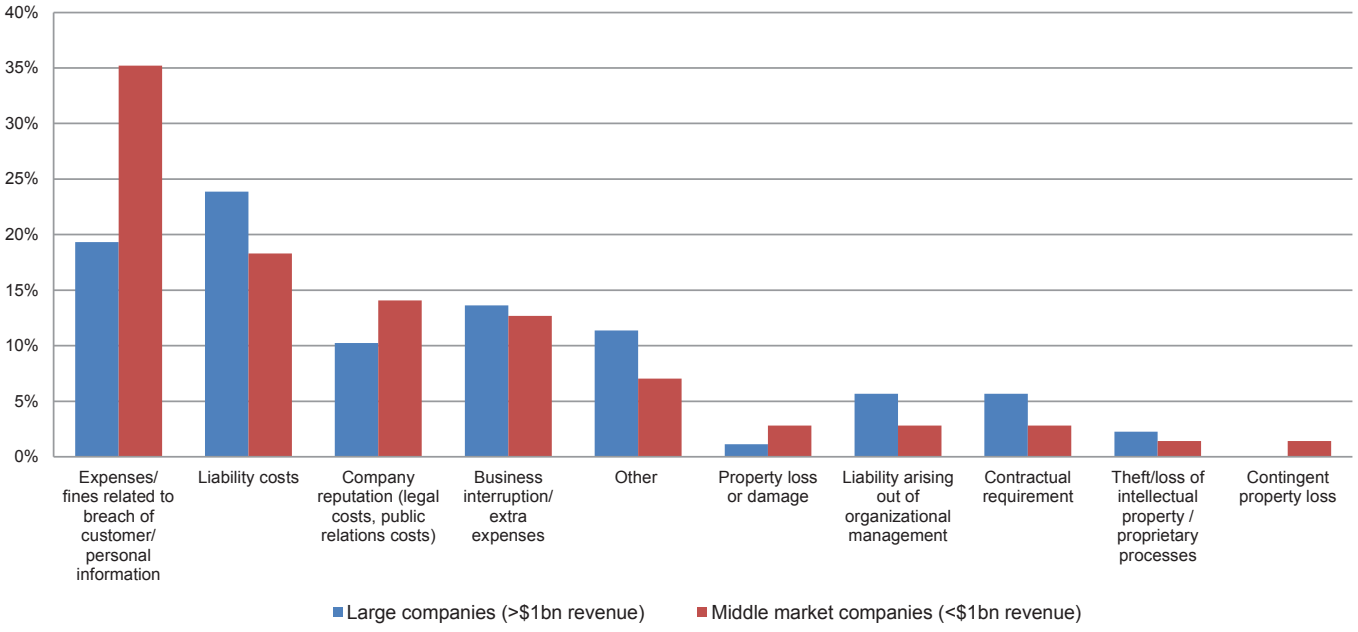
"As we do not do business in the EU, we have not changed our controls," said another middle market respondent.

## HAS YOUR ORGANIZATION MADE CHANGES TO ITS CYBERSECURITY CONTROLS AS A RESULT OF GDPR, A DIRECTIVE MADE EFFECTIVE BY THE EU ON MAY 25?




Another area that illustrates how risk professionals of large and middle market companies were influenced by regulatory changes is with regard to the purchasing of insurance. While regulatory interpretation or uncertainty (e.g., GDPR/PCI/HIPAA) was not the most frequently cited response of either large or middle market companies, significantly more large companies cited it as the primary reason for purchasing cybersecurity insurance than their middle market counterparts.

## WHAT WAS THE PRIMARY REASON FOR PURCHASING CYBER COVERAGE?



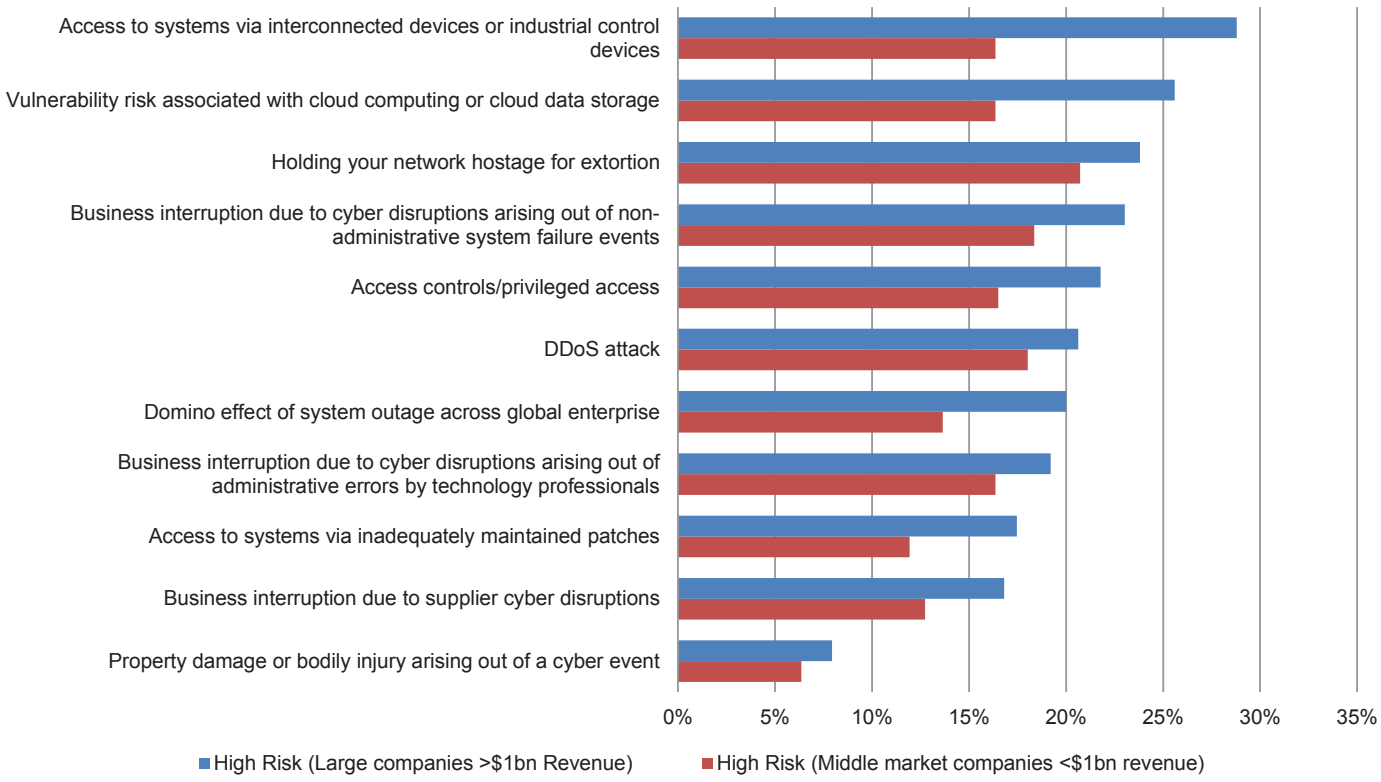
## Large companies view business continuity risks as a greater threat when compared with middle market companies.

High-profile cyber events like the ransomware and malware events in 2017 have brought to light the potential for substantial cyber losses that go beyond data breaches. Respondents were asked to rate two separate sets of exposures — data integrity risks and business continuity risks — on a three-point scale ranging from low risk to high risk. Overall, the study revealed risk professionals remained more concerned about their exposures to data integrity risks than business continuity risks. On average, 33 percent of the respondents rated data integrity risks as "high risk," compared with 18 percent for business continuity risks.

This could indicate that risk professionals are either less educated about the exposures, have concluded these exposures are less significant to their business, or are confident in their cybersecurity controls. The reason could also be that risk professionals are not fully aware that the nature of cyber risk has evolved beyond data security and is moving toward interconnected risks, including business interruption due to malware and ransomware attacks.

The results, however, varied based on company size. On average, 21 percent of large organizations rated business continuity risks as "high risk," compared with 15 percent of middle market companies.

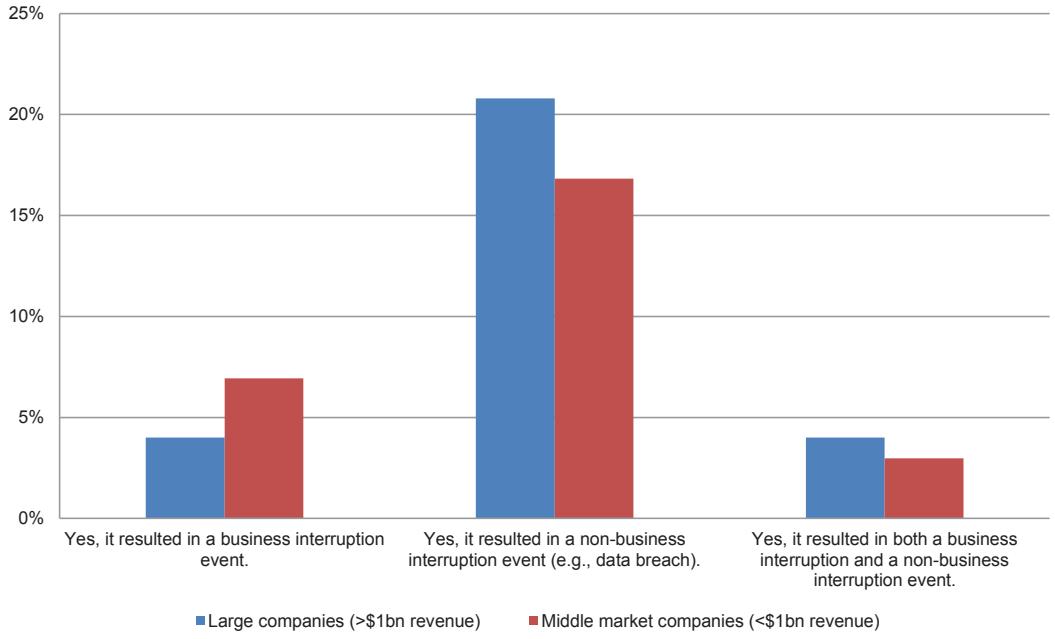
FROM THE PERSPECTIVE OF YOUR ORGANIZATION, PLEASE RATE EACH OF THESE BUSINESS CONTINUITY RISKS.



The cybersecurity controls that a business has in place can be a direct response to a loss they incurred. To better understand the types of losses respondents have experienced, companies were asked if they have experienced a cyber event that resulted in an economic loss.

Interestingly, a similar percentage of large and middle market respondents have been impacted by a cyber event. However, large organizations were more frequently impacted by data breaches and middle market organizations were more frequently impacted by business interruption events. It is possible that this higher frequency of business interruption losses by middle market companies is a direct result of fewer controls implemented to identify, detect, protect, respond and recover from business continuity risks.

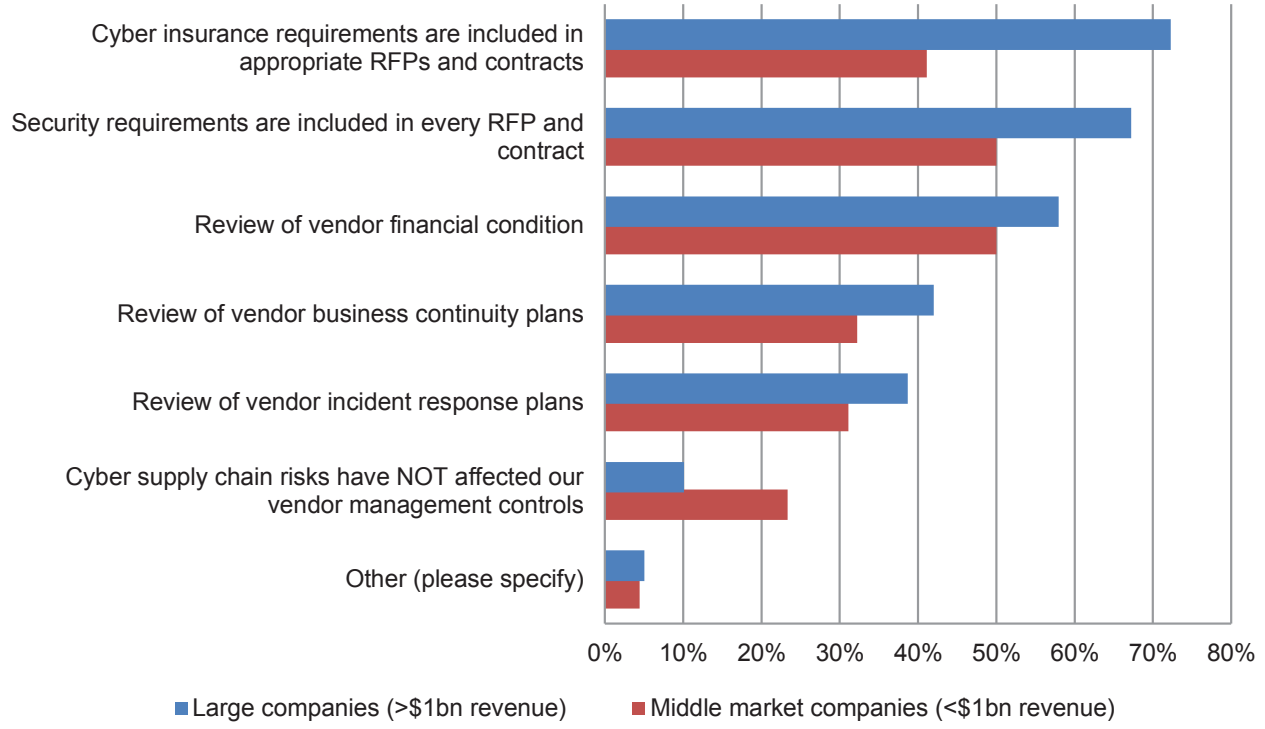
**HAS YOUR COMPANY HAD A CYBER EVENT THAT RESULTED IN AN ECONOMIC LOSS?**




The study also revealed large companies are more likely to mitigate their supply chain risks through the use of a variety of tools available to them. This is consistent with the results that showed they are more concerned about business continuity risks than their middle market counterparts and have experienced fewer business continuity events. Most significantly, 72 percent of large companies include cyber insurance requirements in their requests for proposals and contracts, compared with 41 percent of middle market companies.

72 percent of large companies include cyber insurance requirements in their requests for proposals and contracts, compared with 41 percent of middle market companies.

WHICH VENDOR MANAGEMENT CONTROLS HAVE YOU IMPLEMENTED TO MANAGE CYBER SUPPLY CHAIN RISKS?
*(Please select all that apply)*




## Sophistication regarding risk mitigation and risk transfer continues to vary by company size.

While there is increased awareness of the threats, businesses are left with difficult risk management decisions related to cybersecurity and how best to manage the risks they face — deciding whether they should retain the residual risk of a cybersecurity breach or transfer it through the purchase of insurance.

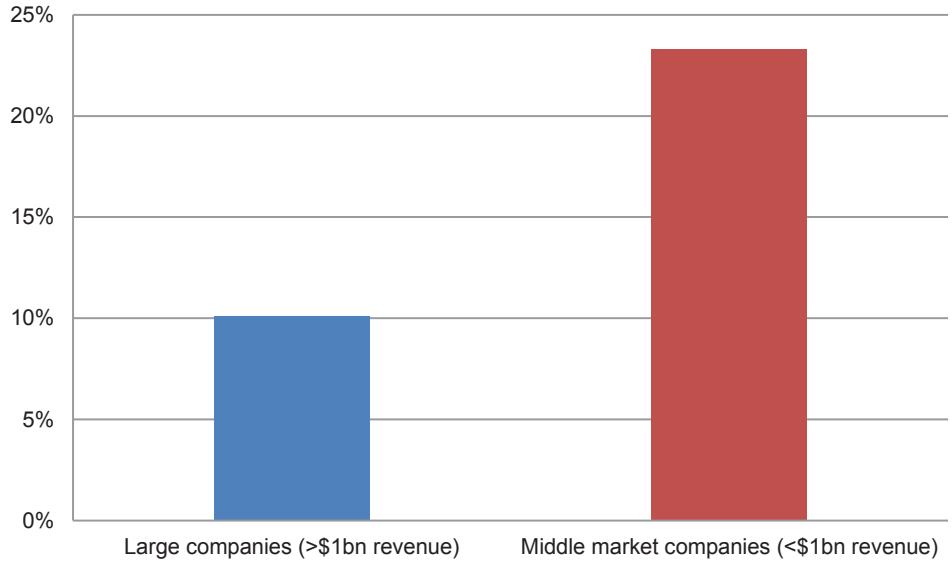
A high level of expertise is required to develop a robust protection, detection, and response strategy that can decrease pressure on a business, lower costs, and help reduce the potential for error. Businesses must adopt a mindset of resilience — rather than just protection — and must encourage a culture of awareness from the board room to the mail room, extending beyond the four walls of the company. Engaging with an insurance carrier or broker's risk management team in an ongoing, comprehensive review of all outside relationships is a key strategy.

An often overlooked aspect of this strategy is the cybersecurity controls of vendors and other business partners. Even companies that make significant investments in cybersecurity find themselves compromised as a result of cybercriminals entering through the "backdoor" (i.e., a company in the supply chain that has access to their systems).

According to the study, more than twice as many middle market companies (23 percent) as large companies (10 percent) said cyber supply chain risks have not affected their vendor management controls. This illustrates another opportunity for insurance professionals to educate their clients regarding how cyber supply chain risk could impact their organizations.

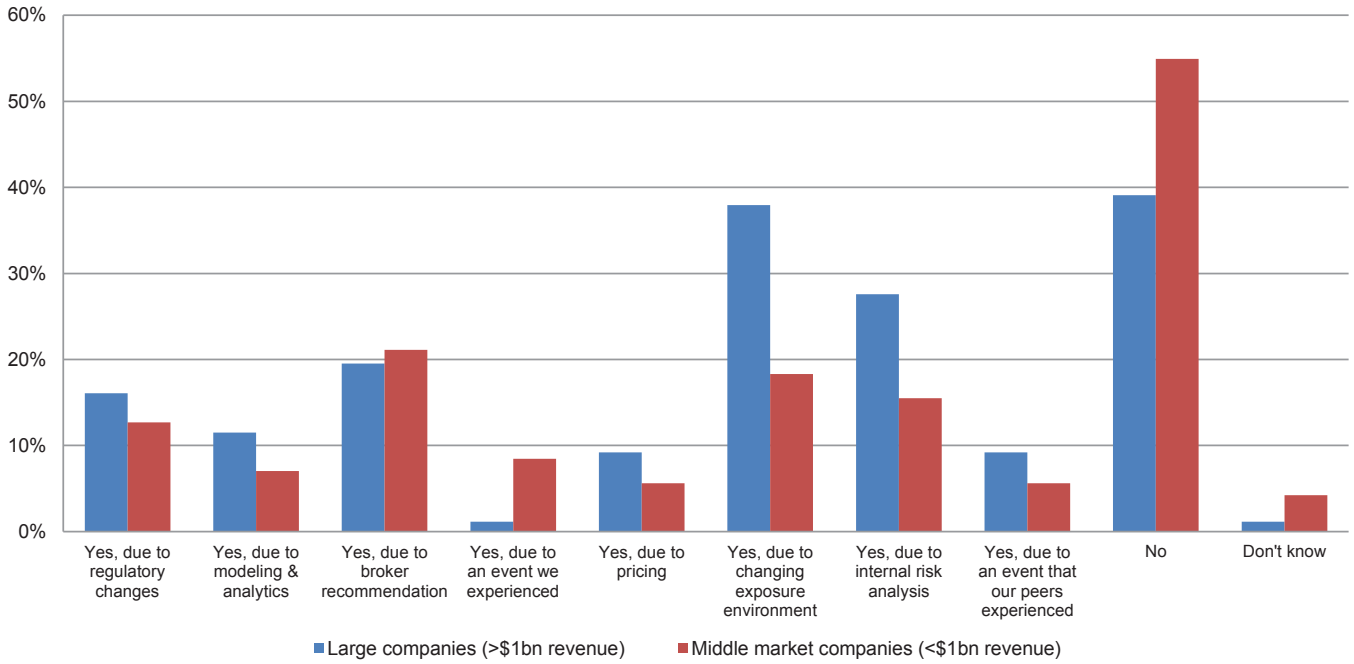
**Businesses must adopt a mindset of resilience rather than just protection; and must encourage a culture of awareness from the board room to the mail room, extending beyond the four walls of the company.**

CYBER SUPPLY CHAIN RISKS HAVE NOT AFFECTED OUR VENDOR MANAGEMENT CONTROLS.



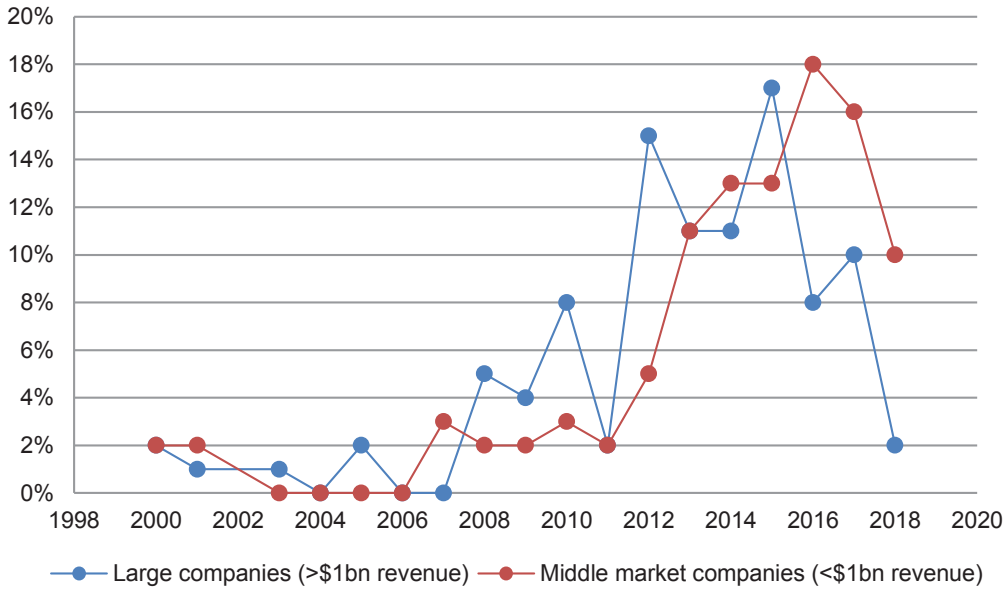

The cyber risk landscape is constantly evolving and therefore often requires a proactive approach to risk transfer to ensure an organization has adequate protection. This is yet another area where large companies demonstrate a higher degree of sophistication than their middle market counterparts. In the past year, 38 percent of large companies have altered their cybersecurity insurance program due to these changes, compared with just 18 percent of middle market companies.

IN THE PAST YEAR, HAVE YOU CHANGED THE STRUCTURE OF YOUR CYBER INSURANCE PROGRAM?
*(Please select all that apply)*



Lastly, until 2015, large companies more frequently purchased cybersecurity insurance to supplement their cyber risk strategies. But over the last three years, a higher percentage of middle market companies than large companies have purchased the coverage. There are a couple possible reasons for this. It could indicate that middle market companies have developed a better understanding of their exposures, or the insurance industry is doing a better job of crafting risk transfer and mitigation solutions that meet the needs of middle market companies.

**WHEN DID YOUR FIRM FIRST PURCHASE CYBERSECURITY AND PRIVACY COVERAGE?**




*2018 figures as of August 2018

## SUMMARY

Taken as a whole, middle market and large companies have different preferences and experiences throughout the cybersecurity value chain. As cybersecurity incidents and concerns continue to evolve, more and more medium-sized businesses have communicated their desire for insurance resources and risk mitigation services to address those concerns. There remains a great need, particularly within the middle market, for education and guidance in developing cyber risk management programs and improving cyber resiliency. The industry is well-positioned to understand those needs and to help develop strategic cyber risk mitigation and response initiatives for the middle market, and to demonstrate the benefits of cyber insurance policies.

## METHODOLOGY

For an eighth consecutive year, Zurich North America and Advisen Ltd. collaborated on a survey designed to gain insight into the current state and ongoing trends in cyber risk management. Invitations to participate were distributed by email to risk managers, insurance buyers and other risk professionals. The vast majority of respondents were from the United States (74 percent), followed by Europe (12 percent), and North America outside the U.S. (7 percent).

The survey was completed at least in part by 313 respondents. The majority classified themselves as either Chief Risk Manager/Head of Risk Management Department (37 percent) or a member of the Risk Management Department (33 percent).

A variety of industries were represented. Finance, banking and insurance had the highest representation, with 26 percent of the total. Other industries with significant representation included manufacturing (9 percent), healthcare (8 percent), educational institutions (7 percent) and technology (7 percent).

The survey was also represented by businesses of all sizes. Overall, it was slightly weighted toward larger companies, toward larger companies, with 54 percent of respondent companies classified as large (greater than $1 billion in revenue) and 46 percent of respondent companies as middle market (less than $1 billion in revenue).