



# »» INFORMATION SECURITY AND CYBER RISK MANAGEMENT

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

OCTOBER

2019

*Sponsored by*



ZURICH®



**Now in its ninth year, Advisen Ltd. and Zurich North America's annual Information Security and Cyber Risk Management Survey demonstrates not only a maturing cyber insurance market, but also better-informed buyers who see the value of cyber insurance. Buyers also know what type of coverage they want and don't hesitate to identify areas where they have discovered new exposures or see the insurance industry as falling short.**

The value of cyber insurance can perhaps be most clearly seen in the survey results which show a more than 70 percent satisfaction rate reported by respondents who have had a cyber claim which either resulted in economic damage or business interruption. This represents a first for the survey – in years past, respondents predominantly had not experienced a cyber claim.

Although more than half of respondents (about 62 percent) feel their cyber insurance meets many of their needs and provides value, many said they have identified gaps in their coverage and overlaps with other lines

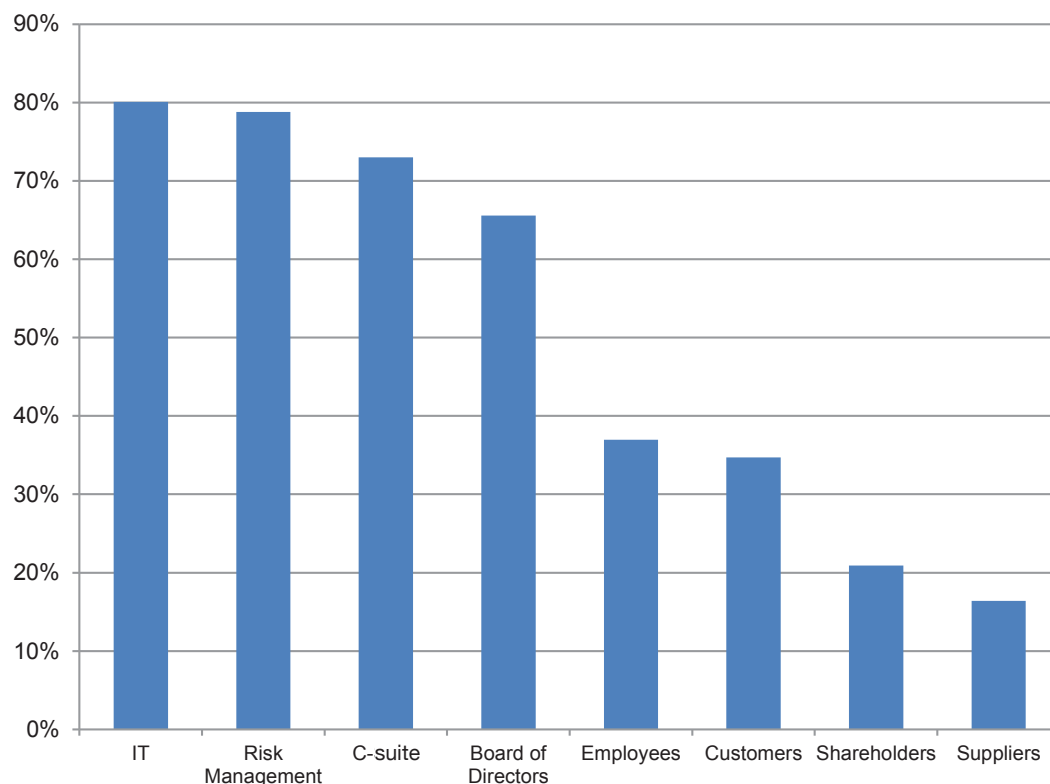
of insurance which should be addressed. This fact speaks to the rising sophistication of buyers as they tie their organizations' risks more effectively to the terms and conditions of their policies.

In terms of what buyers want from their coverage, respondents listed cyber-related business interruption and data breach as the two risks they expect cyber insurance to cover. In fact, business interruption frequently rose to the top of the list for respondents when considering the value of their cyber insurance programs and when thinking about future changes.

## SURVEY HIGHLIGHTS

- Buyers want as much as they can get on their next renewals – higher limits, broader coverage. Seventy-four percent of those who recently changed their coverage said they changed it to buy higher limits in the last year.
- When they have changed their programs, buyers say it was due to changing exposures, internal risk analysis, modeling/analytics, or broker recommendations. This signals an increasing awareness across the respondent base.
- Coverage needs are changing – business interruption needs have come more to the fore for buyers and insurance policies may need to shift in order to effectively meet needs.
- Buyers still predominantly feel cyber insurance policies are not easy to read or understand, nor do they see consistency.
- Buyers are more sophisticated. They know what they want and they know to look for gaps in coverage.
- Buyers tend to be more concerned about losing access to their networks for extortion over other types of cyber risk.
- IT and risk managers are still more concerned about cyber risk than boards and the C-suite
- Expenses and fines related to regulations drove many of the purchases of cyber insurance.
- Nearly one-third of respondents have experienced a cyber claim and over 70 percent reported their claim was covered and they were satisfied with the claims handling process.

### IN YOUR EXPERIENCE, WHICH OF THE FOLLOWING GROUPS VIEW CYBER RISKS AS A SIGNIFICANT THREAT TO YOUR ORGANIZATION?





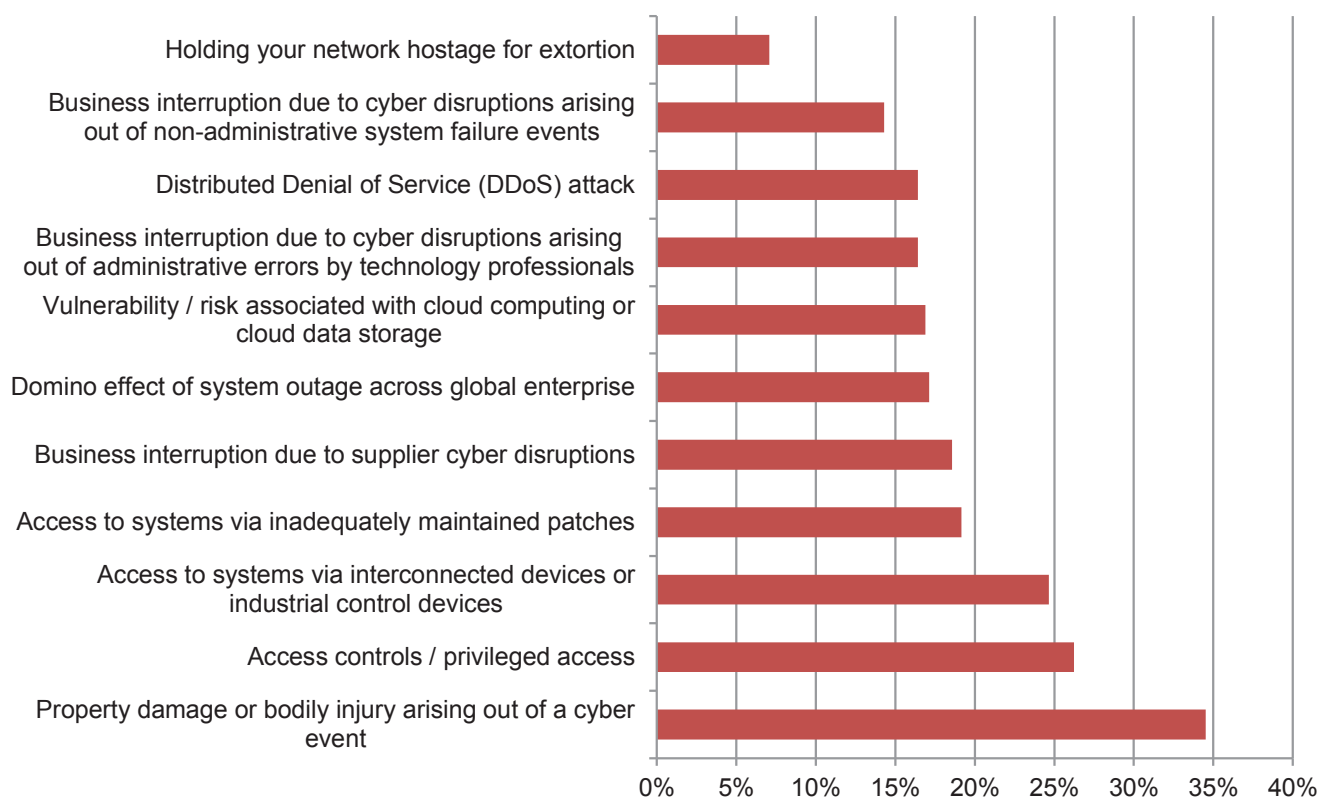
## DISCUSSION OF FINDINGS IN DEPTH

### Business interruption is a key concern for buyers

Respondents show keen interest in having their cyber policies cover business interruption – 95 percent said they expect it will be covered in their cyber policies in the event of a claim. Seventy-five percent of respondents also say they expect contingent business interruption to be covered, reflecting awareness that cyber breaches or disruptions at third-party vendors can have negative effects as well as first-party business interruption.

Respondents showed significant concern for most business continuity risks. However, breach of customer records and malware intrusions are still more of a worry — nearly 40 percent cited breach of customer records or malware intrusions as “high risk” compared to 30 percent citing “holding your network hostage for extortion” as a high risk.

**FROM THE PERSPECTIVE OF YOUR ORGANIZATION, ON A SCALE FROM ONE TO SIX, PLEASE RATE EACH OF THESE BUSINESS CONTINUITY RISKS.**



Respondents' increased understanding of business interruption as a risk reflects growing awareness that cybercriminals do not discriminate by size, location, or industry. Even organizations which do not collect customer data can find themselves experiencing cyber-related disruption.

## Coverage in demand

Responses to most-wanted coverages clearly reflected the last 12 to 18 months where ransomware attacks dominated the news. Choosing from a list which included 11 possible outcomes of cyber risk, 95 percent of respondents named data breach as the number-one risk they expect to be covered by their cyber insurance. It was closely followed by cyber-related business interruption at 94.5 percent and cyber extortion/ransom at 89 percent. As one respondent put it, “this is what I would want MY cyber policy to cover.”

This comment along with the strong showing of support for business interruption and cyber extortion to be covered offers an action item for both buyers and the insurance industry. Such cover is readily available in the marketplace, but it falls to buyers and their brokers to ensure that their perceptions of what their policies cover match the reality.

Nearly 78 percent said they believe business interruption is covered by their policy, with about nine percent indicating it is covered under another policy and five percent saying they would be interested in buying the coverage. Another nine percent did not know whether business interruption is covered under their cyber policy.

The increasing awareness of the limitations of property coverage and hardening of the property market is influencing and accelerating a maturation of the cyber business interruption market. Historically, property insurance policies offered higher limits for business interruption for covered property damage. Buyers now want to see similar limits for business interruption coverage on their cyber standalone policy.

This clear market demand may drive the standalone cyber market to refine their offerings, bringing cyber-related business interruption limits up to the level of standard property forms.

The survey results show insurance buyers see both a potential gap in limits of coverage as well as overlaps of coverage – 36 percent believe they have cyber-related property damage/bodily injury coverage under another policy. This reflects the belief that some coverage for cyber as a cause of loss can be found under traditional policies.

With nearly 60 percent of respondents expressing concern about perceived gaps and overlaps in their insurance coverage, buyers have sent a clear message calling for policy clarity. Buyers also have a long list of coverages they would like to see – some want bricking cover (coverage for hardware or devices that have been damaged beyond repair), others want “full limits” for social engineering claims, and many commenters say they want more extensive coverage for incident response.

Thus, respondents are seeking “a clearer differentiation between cyber and monoline policies” and “definitive clarity on events insured and not insured.”

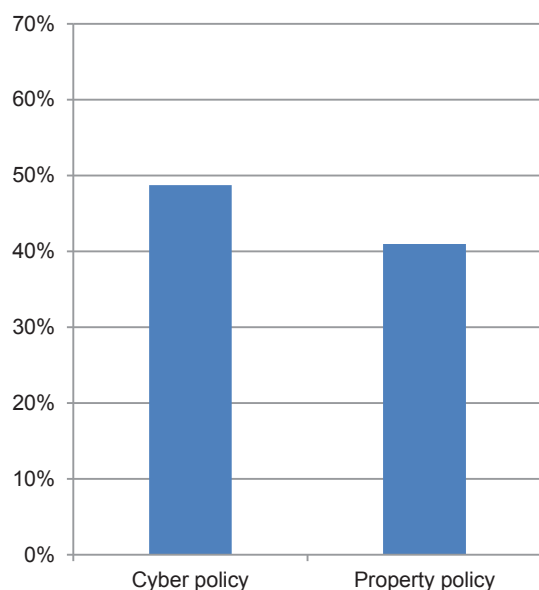
**The hardening of the property market is influencing and accelerating a maturation of the cyber business interruption market.**

## Now leaving the property market

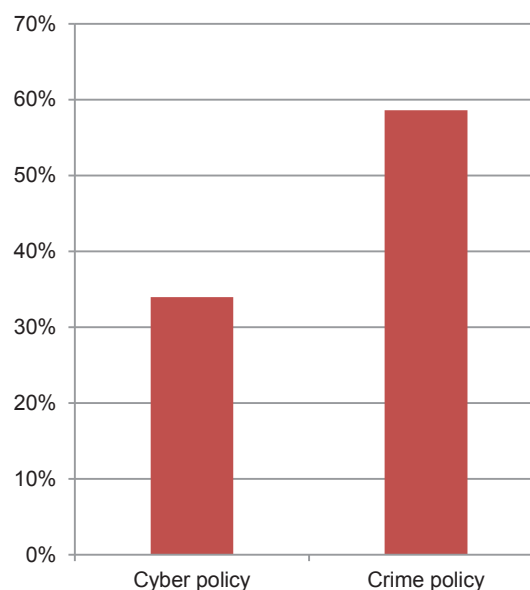
In asking respondents about the two most common areas of overlap on coverage – crime and property – buyers generally feel most cyber-related property damage should be covered by a standalone cyber policy. However, in terms of funds transfer fraud losses, respondents look more to their crime policies to cover the resulting financial losses.

The results were only by a small margin for cyber-related property damage (49 percent to 41 percent in favor of cyber policies). Respondents were more divided on crime versus cyber (59 percent for crime compared to 34 percent for cyber). Comments from respondents offer more insight into how buyers would like to craft their coverage to address these risks.

### WHERE DO YOU BELIEVE COVERAGE BELONGS FOR CYBER-RELATED PROPERTY DAMAGE?



### WHERE DO YOU BELIEVE COVERAGE BELONGS FOR A FUNDS TRANSFER FRAUD LOSS DUE TO SOCIAL ENGINEERING?



Buyers report that they are migrating away from covering cyber-related damage on monoline property policies because of their increasing awareness that standard property policies cover only limited aspects of computer-related losses. Several respondents suggested they would prefer third-party liability property damage to be on their cyber policies, with first-party coverage for property damage like bricking on a property policy. Multiple respondents also stated they would like to see some coverage under their commercial general liability policies for property damage. However, confusion and inconsistency of appetite in this arena persists, as demonstrated by these responses.

Some respondents believe they have coverage under both cyber and property policies – over one-third of respondents said they do have cyber-related property damage and bodily injury coverage under a policy other than their cyber policy.

For funds transfer fraud losses, the majority of respondents believe coverage should be found under the crime policy, but also state they would like to be able to recover under both crime and cyber policies or have separate policies with higher limits.

### Regulatory impact

In addition to the widening impact of ransomware attacks, few topics occupied cyber headlines last year like the significant regulatory fines and penalties against major companies which have experienced breaches. As reported, the record fines under the European Union's General Data Protection Regulation (GDPR) against British Airways and Marriott International served as a major wake-up call – one which has been heard loud and clear by respondents to our survey. Up until the \$230 million British Airways fine and the \$123 million Marriott fine, penalties under GDPR had been modest, with even the French data protection authority's \$57 million fine against Google seeming like little more than a slap on the wrist. These latest fines signal the intention of European data regulators to wield their authority more sternly and insurance buyers now want to know how their cyber coverage will respond.

**Over 35 percent said they bought coverage expressly to cover fines and expenses due to breach of customer data, an increase from last year.**

A significant majority – 71 percent – say they expect their cyber insurance to cover regulatory fines and penalties. Over 35 percent said they bought coverage expressly to cover fines and expenses due to breach of customer data, an increase from last year, when 26 percent said fines and penalties motivated their purchase.

Multiple respondents said they want clarity on whether fines and penalties are covered on next renewal, and approximately 15 percent said they made changes to their cyber insurance program this year as a direct result of increased risk of regulatory actions. One commenter stated, "I consider that the cyber insurance products are still evolving and currently don't provide the cover we are looking for. Th[ere] is still uncertainty over whether GDPR fines would be covered and this is currently our major risk."

In past years, GDPR has dominated the regulatory arena – in this year's survey, respondents cited the upcoming California Consumer Privacy Act as a concern. The law, which will be implemented in 2020, bears some similarities to GDPR in terms of consumer control over data and promises wide-ranging consequences for businesses which run afoul of the law.

Other states show signs of following California's lead on consumer data privacy legislation, which means insurers and brokers will need to be ready to provide clarity on coverage. In addition to CCPA, the Illinois Biometric Information Privacy Act (BIPA) promises increased litigation and regulatory action. In August 2019, the U.S. Court of Appeals for the Ninth Circuit allowed a class-action lawsuit against Facebook to proceed, with plaintiffs alleging the social media giant violated class members' privacy rights under BIPA. In addition to watching this area from an enterprise risk management perspective, businesses also seek a determination of whether associated costs will be insurable.

## Cyber insurance pays claims, per the results

An overwhelming majority of respondents (nearly 70 percent) which had filed a cyber insurance claim reported they were either “satisfied” or “very satisfied” with the outcome of their claim. Seventy percent also said their claims were covered by their standalone cyber insurance policy. With consistent questions from outside the insurance field about whether cyber insurance pays out for claims, the survey results clearly indicate that, yes, it does.

New for this year’s survey, we asked respondents to discuss their experience with the cyber claims process in more depth. In last year’s survey, 73 percent of respondents had not experienced a cyber event. That number shifted slightly with this year’s results, with 30 percent having experienced an event which caused either economic loss or business interruption.

The satisfied customers in our survey offered both compliments and advice for the claims handling process. One respondent noted, “It was a huge benefit to our organization to have an insurance partner that was able to bring talented subject matter expertise to walk us through our data breach situation.” Another praised the “excellent” response team on their case.

However, the survey results also revealed some areas where buyers may still need guidance. Numerous respondents said they experienced claims which would have fallen within the terms and conditions of their policies, but fell below their retention levels. One commenter said, “Our cyber-breach was not large enough to receive the benefits we thought we would receive” and this was not an uncommon experience. It appears the trade-off for buyers seeking higher limits may be greater retention. This is an equation organizations need to revisit as they look at their cyber event experience and make the case for buying coverage in the future.

Respondents also expressed frustration with some of the claims handling timelines – one commenter called the process too “immature” to handle claims in a timely fashion. Respondents also cited the need for local response teams to have forensics on the scene quickly.

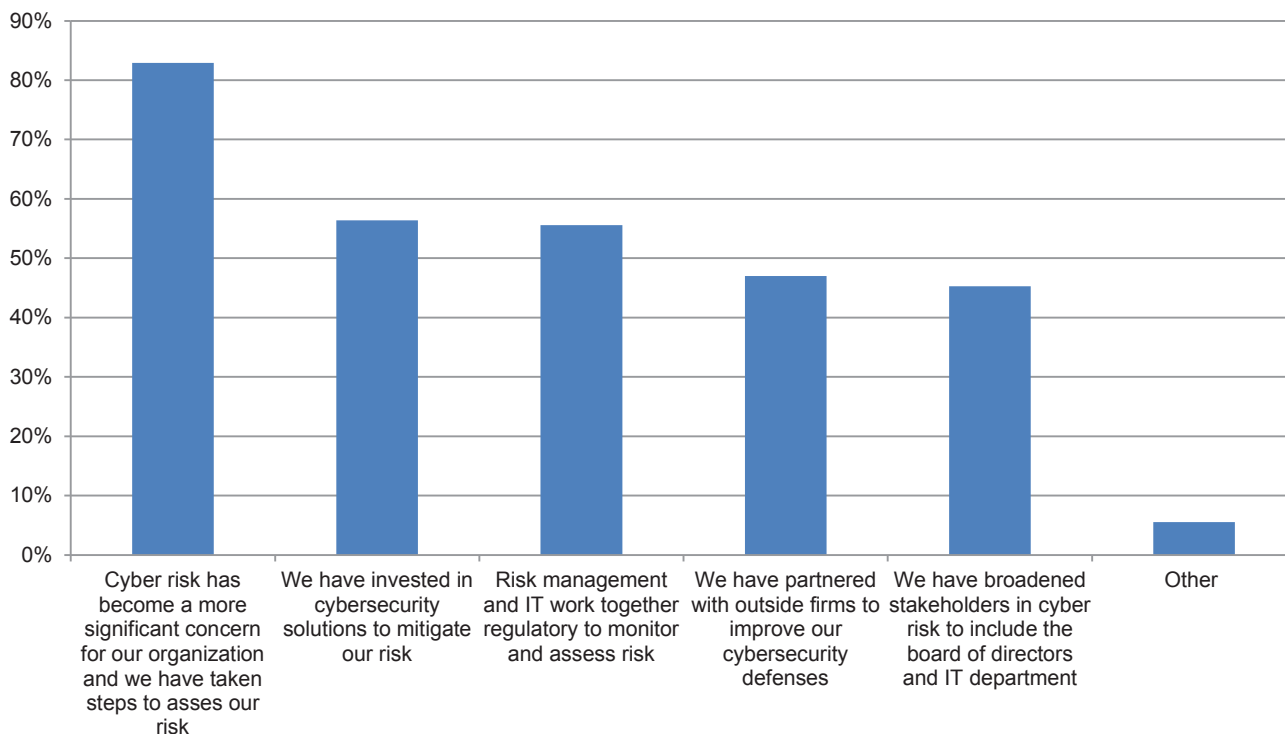
## Evolution of the cyber insurance market: more sophisticated buyers

As we noted, the insurance buying market has increased in sophistication and sees the value of cyber insurance. The vast majority of respondents (82 percent) state cyber risk has become a significant concern across their entire organization. The responses show it doesn’t stop with “concern” – organizations are putting in the work, hiring CISOs, buying cyber insurance, working with outside firms to assess their cyber risk, and conducting tabletop exercises to test their breach response plans. This should be welcome news to the insurance industry, along with the fact that 63 percent said they have updated their privacy and network security processes and taken other steps to secure their sensitive information.

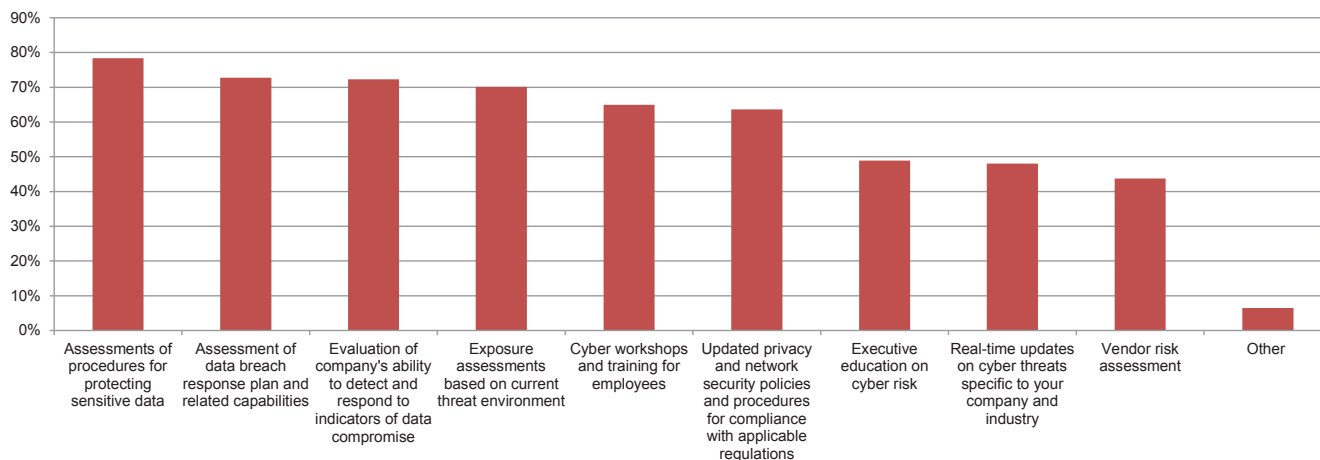
**With consistent questions from outside the insurance field about whether cyber insurance pays out for claims, the survey results clearly indicate that, yes, it does.**



## HOW HAS YOUR ORGANIZATION'S APPROACH TO CYBER RISK MANAGEMENT EVOLVED OVER THE YEARS?



## MY ORGANIZATION'S CYBER RISK MANAGEMENT PLANS INCLUDE:



Respondents indicated they conduct employee training on cyber risks, predominantly on an annual basis (40 percent). One respondent explained their reasoning: “95 percent of security breaches are due to human error, and that is the number one thing that companies need to internalize and protect against, especially on the social engineering side.”

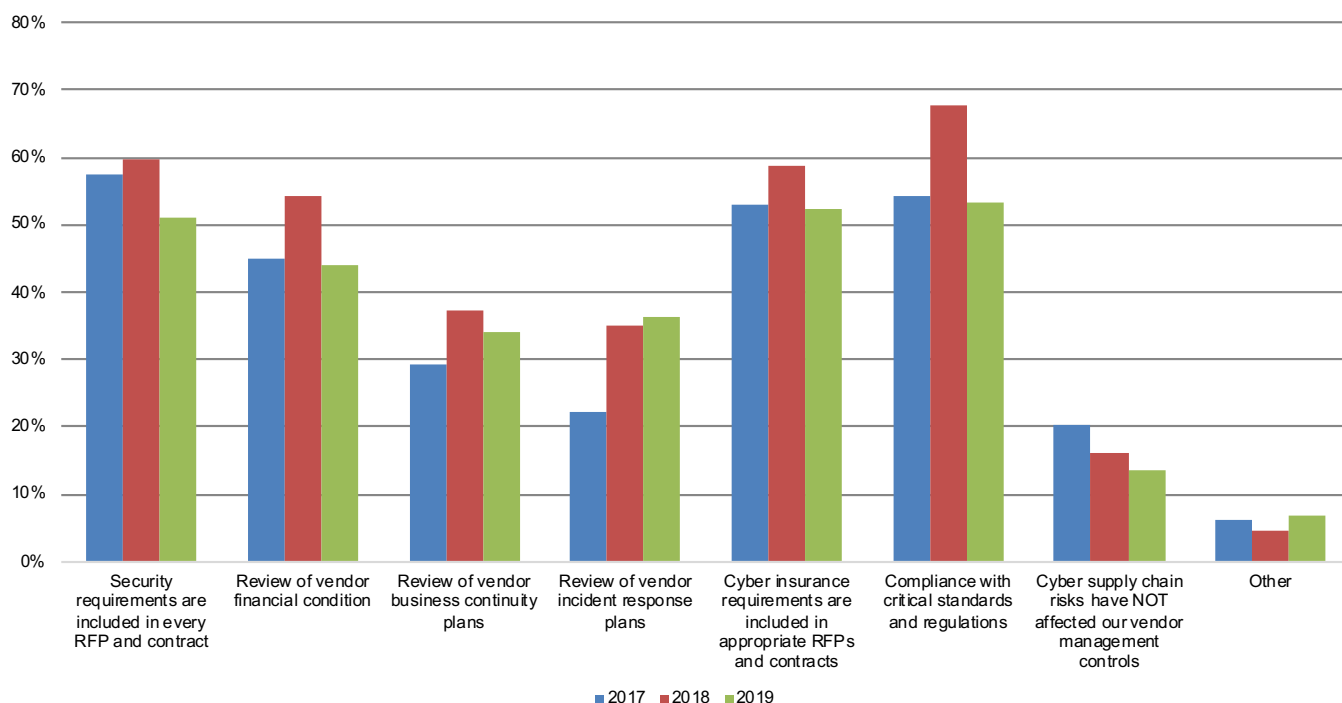
## Not enough focus on third-party risk

Just over half (51 percent) of respondents have security requirements in every request for proposal (RFP) and contract for outside vendors, a slight drop from last year's results of 59 percent. Similarly, although 59 percent of respondents to last year's survey required their vendors to carry cyber insurance, the number dropped to 52 percent this year. Even the dedication to ensuring vendor compliance with critical standards and regulations dropped from 68 percent to 53 percent.

In fact, attention to vendor management controls dropped overall in the 2019 survey, a worrisome trend as third-party risk can cause not only supply chain issues, but often provide cybercriminals an indirect route into larger organizations with more sensitive information. With the number of breaches caused by access through a third party – dating back to Target's 2013 breach – these precipitous drops in buyer attentiveness in just one year are problematic. The comments section for questions related to vendor risk management should raise a red flag for any insurer: "I don't know," "None of the above," "Nothing extensive on vendors," and "Unsure."

Attention to vendor management controls dropped overall in the 2019 survey, a worrisome trend as third-party risk can cause not only supply chain issue, but often provide cybercriminals an indirect route into larger organizations with more sensitive information.

### WHICH VENDOR MANAGEMENT CONTROLS HAVE YOU IMPLEMENTED TO MANAGE CYBER SUPPLY CHAIN RISKS? (Select all that apply)



Multiple comments indicated that insureds would like to see more focus from their insurance partners on third-party risk, signaling that businesses want insurers and brokers to take the lead on helping to manage this increasingly critical cyber risk.

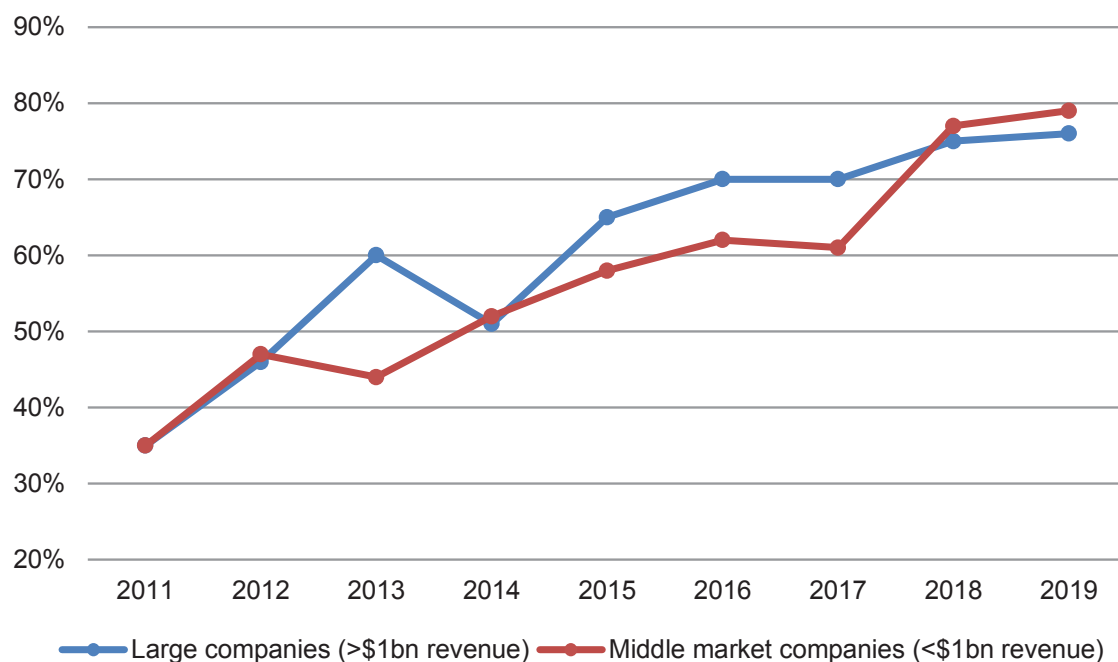
## Insurance buying soars

Cyber insurance take-up rates are improving. Over 70 percent of respondents buy cyber insurance, with nearly 60 percent buying standalone cyber policies, an increase from last year as buyers come to realize that dedicated cyber coverage can be customized to meet individual needs. Others buy it as part of their professional liability program or via endorsement. However, 14 percent of respondents do not buy cyber, and 8.8 percent said they did not know whether their companies have coverage. Eighty percent of non-buyers have considered it, but cite lack of knowledge, cost versus benefit, and “lack of IT buy-in” as reasons for not purchasing cover.


The take-up rate of coverage will likely increase further, as businesses learn more and as coverage evolves. Attitudes toward and involvement with cyber risk management have shifted, including the fact that IT and risk management still rank highest on concern for cyber risk within the organization – but they are closely followed by the board and C-suite. Since 2011, the inclusion of boards and C-suite executives in cyber risk decision-making has risen from 45 percent (directors) and 58 percent (C-suite) to 66 percent and 73 percent, respectively.

Results show most respondents began buying cover in 2015, followed by 2017 or 2016. The reasons given included taking a proactive stance, cyber exposure to all of the listed reasons, and notably, seeking to protect their reputation.

### EIGHT-YEAR CYBER INSURANCE PURCHASING TREND



However, even with buyers' sophistication levels rising, over 40 percent of respondents still either disagree or completely disagree with the statement “Cyber insurance policies are written in a clear and easy-to-understand manner.” As one commenter noted, “There is still a major gap in knowledge ...



jargon and techspeak make the cyber world seem esoteric and hard to understand, so people put it in the ‘too hard’ basket too often or simply assume their IT person will be on top of it.”

Others offered similar commentary, stating “cyber insurance policies are changing at a rate which is difficult to keep up with” or “need more consistency in policy language.”

For every “needs more clarity” comment, though, there are opposing views. One respondent told us, “The cyber insurance market has made purchasing this coverage easier over the years. The applications are easier to understand and complete. The carriers are offering coverage that offer more options and resources to deal with claims than they have in previous years.”

Other commenters are more succinct: “Cyber insurance is a necessity and part of the cost of doing business in this day and age.”

### Projections for the future

With such a clear interest shown in cyber-related business interruption coverage and respondents’ clear preference for having this under a cyber policy versus property policies, the cyber market is due for a change in how it approaches business interruption.

In order to be of more value to buyers, the cyber policy’s business interruption coverage may need to evolve in sophistication, becoming more like the business interruption coverage available for other perils.

Respondents say they want more cost-effective capacity from the market and greater attention to industry-specific risks. More than one buyer termed coverage as too “generic” or “not adequate” to meet their specific needs. This may be the result of coverage developing from a data breach notification product aimed at traditional data holders, but as the customer base, the coverage must as well. As one respondent noted, “Current coverage offered by the market is OK for retailers or others that customers avoid after a breach (i.e., I’m not shopping at Target or staying at a Marriott), but doesn’t really work for companies like mine — real estate, leases in place, so no immediate revenue drop, but may not be able to secure new tenants due to breach.”

As buyers’ maturity grows, they would also like to see the same from the cyber insurance side in terms of discounts for proactive risk mitigation, better expertise on the part of brokers, and uniform global standards to “strengthen and expand the cyber risk insurance market and reduce cyber risk.”

“We do not get credit from the market for having highly advanced cybersecurity measures in place. We have invested a great deal of time and money to bring ourselves up to world-class standards, but the underwriters do not differentiate,” said one commenter.

Managing customer expectations, risk aggregation, and meaningful coverage enhancements remain goals for all segments of the cyber insurance market. The overlaps of cyber risk with other lines of insurance suggest a continued focus on eliminating uncertainty is needed – while ensuring customers can procure coverage for cyber risks in a way which makes sense for their organizations’ individual needs.



One commenter saw a way forward for the insurance industry through technology, noting “The quality of the cyber insurance coverage in the market is a direct reflection of the different carriers in the market and of the tools and analytics they are putting to use in order to assess the risk profile of their insureds. As carriers become more adept at utilizing technology tools to build the risk profile of their insureds, they will rely less on the traditional insurance application process.”

## Methodology

For nine consecutive years, Zurich North America and Advisen Ltd. have 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 (79 percent), followed by Europe (10 percent), and North America outside the U.S. (4 percent).

The survey was completed at least in part by 350 respondents. The majority classified themselves as either Chief Risk Manager/Head of Risk Management Department (29 percent), a member of the Risk Management Department (22 percent), Executive (CIO, CEO, CFO, CISO, or chief privacy officer) (22 percent) or other risk professional engaged in the buying process (27 percent).

A variety of industries were represented. Finance, banking and insurance had the highest representation, with 42 percent of the total. Other industries with significant representation included manufacturing (7 percent), healthcare (5 percent), technology (8 percent), and educational institutions (3 percent). The “other” category represented 12 percent of respondents, many of whom indicated they were from nonprofit organizations.

Businesses of all sizes responded to this year’s survey. Smaller firms with less than \$25 million in revenue comprised the largest share (24 percent). Larger businesses (greater than \$1 billion in revenue) represented 43 percent of the respondents, but the majority of respondents came from smaller and middle market companies (less than \$1 billion in revenue) at 57 percent.

*Disclaimer:* The information in this publication was compiled from sources believed to be reliable for informational purposes only. All sample policies and procedures herein should serve as a guideline, which you can use to create your own policies and procedures. We trust that you will customize these samples to reflect your own operations and believe that these samples may serve as a helpful platform for this endeavor. Any and all information contained herein is not intended to constitute advice (particularly not legal advice). Accordingly, persons requiring advice should consult independent advisors when developing programs and policies. We do not guarantee the accuracy of this information or any results and further assume no liability in connection with this publication and sample policies and procedures, including any information, methods or safety suggestions contained herein. We undertake no obligation to publicly update or revise any of this information, whether to reflect new information, future developments, events or circumstances or otherwise. Moreover, Zurich reminds you that this cannot be assumed to contain every acceptable safety and compliance procedure or that additional procedures might not be appropriate under the circumstances. The subject matter of this publication is not tied to any specific insurance product nor will adopting these policies and procedures ensure coverage under any insurance policy. ©2019 Zurich American Insurance Company. All rights reserved.