Advisen
Transforming • Insurance™

PartnerRe

2017 SURVEY OF CYBER INSURANCE MARKET TRENDS

PartnerRe & Advisen

For the fourth year, PartnerRe has collaborated with Advisen to undertake a comprehensive survey of the evolution of the market for Cyber insurance, both first- and third-party coverage, and the factors and trends impacting that evolution.

The 2017 Survey of Cyber Insurance Market Trends

This whitepaper is based on the survey responses and comments of 270 brokers/agents and 125 underwriters from around the world, all directly involved in Cyber insurance business.

We sincerely thank everyone who contributed; without their assistance, this survey's outcomes, some of which are of particular interest, would not have come to light.

NEW *for* 2017

This 2017 survey tracked the same aspects of Cyber risk and coverage as in previous years, such as identifying the top drivers of Cyber insurance sales, the leading factors influencing buying decisions, and the biggest obstacles to placing coverage. New for 2017, the survey included additional questions which produced notable results:

- To better understand buying habits, we asked respondents if they had observed existing Cyber insurance business switching from endorsement to stand-alone policies: 84% said they had, an indication that endorsements might be a good way to introduce Cyber insurance coverage to new buyers.
- Two cyber events happened as we were preparing the survey questions: the Dyn DDoS attack in the third quarter of 2016 and the WannaCry Ransomware attack in May 2017. We asked whether these events had had an impact on Cyber underwriting and/or pricing: Surprisingly, over 45% of respondents said "No impact."
- Given the many references to cyber-related property damage (PD) in our 2016 Survey, we asked whether this coverage belonged under a Property policy or a Cyber policy. Overall, the market was split; however, when we took a closer look at the numbers, underwriters felt more strongly than brokers that the risk belonged under a Property policy.
- We asked respondents about the source of Cyber business by territory. Non-U.S. growth was apparent: About 24% of respondents reported sourcing at least half of their Cyber insurance business from outside the U.S.

Key findings at a glance

According to **62%** of brokers, Cyber coverage is becoming more consistent, but it is still difficult to compare policies

The Dyn DDoS attack and WannaCry ransomware attack had slight to no impact on underwriting and/or pricing for **71%** of respondents

Pricing is seen as less consistent than last year, many brokers noting soft market conditions and broadening coverage without adequate rate consideration

Healthcare still leads the new buyers list, but other industries are catching up

Market expands as existing insureds continue to buy more coverages and higher limits at renewal

News of a loss continues to be the main driver for Cyber insurance sales

Over **80%** noted buyers switching from Cyber endorsements to stand-alone policies - **43%** noted that this occurred frequently

Market was split on whether cyber-related property damage should be covered by a Property policy (44%) or a Cyber policy (40%)

More than half the respondents felt that social engineering losses (funds transfer fraud) should be covered under a Crime policy

24% of respondents felt that the GDPR would have a significant impact on the take up rate of Cyber insurance in Europe

Not understanding the exposures and coverage remained as the main obstacle to selling Cyber insurance

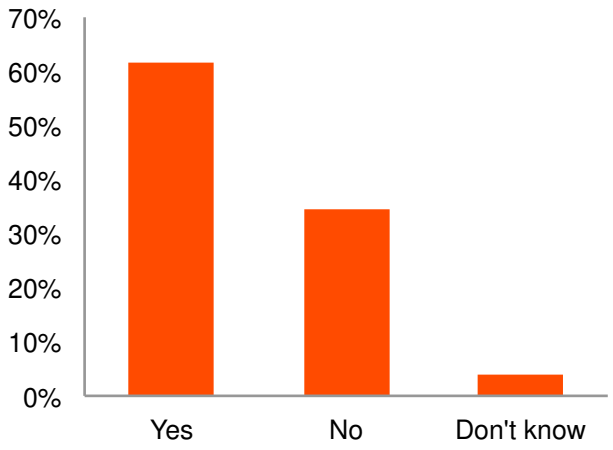
COVERAGE, PRICING, AND AGGREGATION MANAGEMENT

This year respondents noted soft market conditions, less divergence in policy forms, and very little impact from significant cyber events.

Coverage is becoming more consistent

Not seen in previous years, responses included unmistakable signs of coverage standardization in the market; 62% of broker respondents feel that Cyber coverage is becoming more consistent among carriers, significantly higher than last year's figure of 38%.

Is Cyber insurance coverage becoming more consistent among carriers?



As regards specific commentary, there were some common themes. Some brokers felt that "coverages are starting to become kind of commodities because of market copy paste efforts," and "as direct markets attempt to get new forms filed, things are improving and becoming more consistent."

Many brokers felt that it was less about coverage differences, and more about terminology. Respondents noted that "the terminology still varies," however, "most carriers tend to have the same coverage, but are labeled with different terms," or more precisely "inconsistency between words and language."

"General areas of coverage are the same, but wordings and product differentiation [are] still hard to map."

And others still felt that "we have a long way to go here" and there still remains an "inconsistency between words and language."

"While markets are starting to be more consistent in coverages offered as they pertain to Cyber, there is still a very wide variety."

For some brokers, standardization of the Cyber form would not be ideal, as one noted that "each carrier's forms and endorsements being unique gives a competitive edge to a Cyber-savvy broker who can manuscript a comprehensive Cyber product for insureds."

"While markets are starting to be more consistent in coverages offered as they pertain to Cyber, there is still a very wide variety."

Brokers placing business with up to six partners

Almost 80% of surveyed brokers generally work with six or less primary insurers. Combined with the responses and commentary to our questions about standardization, these results may suggest a preference to remain with familiar insurers and policy forms.

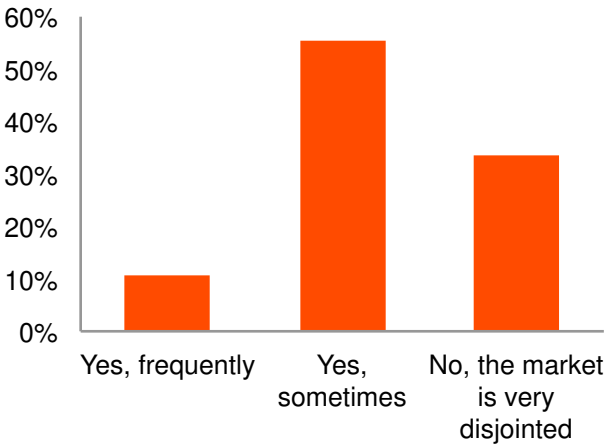
Competition is driving pricing

Competition between carriers was seen to prevail over actuarial assessment of the cost of risk. One respondent noted it's "becoming a sales game, rather than the pricing of risk. This is causing a perpetually softening market."

Brokers are finding the market a little less consistent in its approach to pricing than last year. Many commented on the broadening of coverage without adequate rate consideration.

"The market is unjustifiably soft right now. This creates an arms race that requires carriers to offer more coverage for lower premiums. It is not a very healthy system that is leading to hardening in specific classes of business."

Is Cyber insurance pricing becoming more consistent among carriers?



"The market is very soft, with most specialty carriers willing to negotiate premium and coverage for the most lucrative classes of business."

"Pricing and competitive features of policies are driving the market in the wrong direction. Some carriers are irresponsible about underwriting to the real exposures."

"Underwriters are giving in to market pressure to provide much broader coverage for lower and lower premiums."

Another comment concluded that, with rapid growth and falling rates, the market for Cyber insurance was approaching a "perfect storm" that could result in widespread underwriting losses. "When will the market identify the confluence of these negative factors?"

Minimal impact of aggregation management on underwriting and pricing

Underwriters were asked if the aggregation of cyber risk was actively managed on a day-to-day basis; more than three-quarters responded "yes."

However, while this might impact some aspects of underwriting, it is clear from the previous section that it hasn't impacted coverage offering and pricing. This is further supported by responses to a question we asked regarding recent events.

When asked if two major cyber events of the last 12 months (see side box) had impacted underwriting and/or pricing, 47% of respondents indicated that there had been "no impact," despite the associated widespread disruption and economic losses of these cyber attacks. About 24% noted that there was a slight impact. Only 2% felt that the impact of these events was significant.

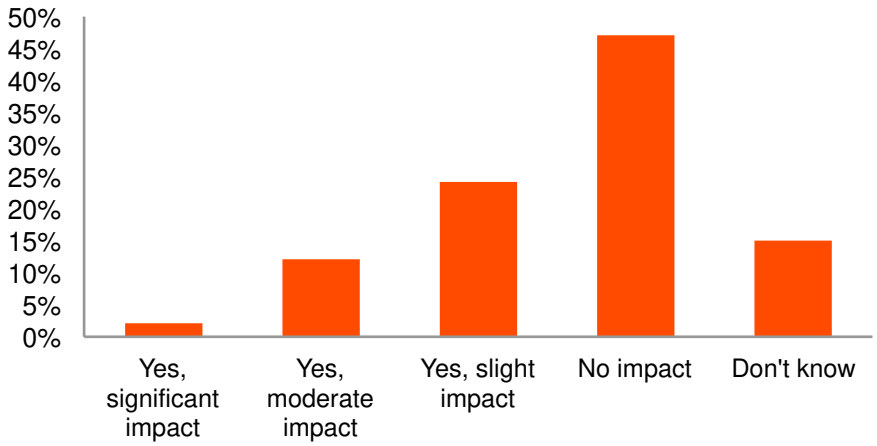
MAJOR CYBER EVENTS OCCURRING AROUND THE TIME OF THIS SURVEY

1. **The distributed denial of service (DDoS) attack in the third quarter of 2016. This attack was made on the domain name provider Dyn, limiting access to some of the best-known websites.**
2. **The "WannaCry" ransomware attack in the second quarter of 2017. This severely disrupted businesses and public sector operations in several countries.**
3. **The questions were completed before the "NotPetya" cyber attack in June 2017, but the survey was administered after the attack. "NotPetya" is a destructive wiper malware that caused significant business interruption to several large multinationals.**

Note, at the time of survey close, no known insured losses of significance were attributed to any of these cyber attacks.

So, despite active portfolio management and the markets' concerns over aggregation, the survey's results could indicate that in the absence of significant insured losses, competitive pressures are driving the pricing of the product for now.

Have systemic events such as Dyn DDoS attack and WannaCry ransomware impacted underwriting and/or pricing?

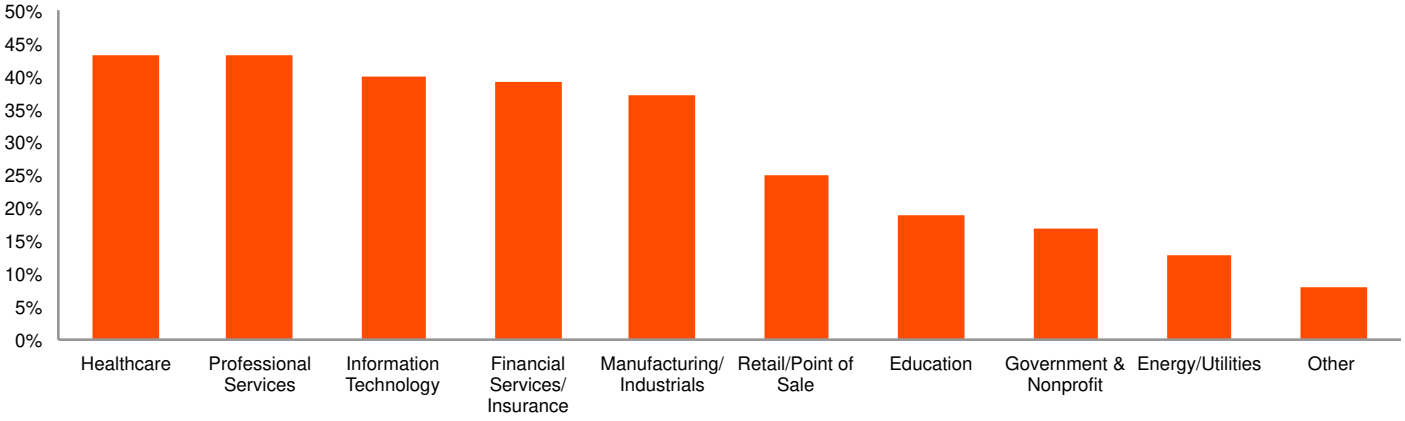


BUYER BEHAVIOR

Shift in new buyers of Cyber

We asked which industries are contributing the most new buyers of Cyber insurance. The healthcare and professional services sectors continue to be the most commonly cited sources of new Cyber insurance buyers.

What industries bring the most New-to-market buyers of Cyber insurance? (Please select top three)



However, results indicate a narrowing of differentials between the top five new business contributors. This might be attributable to an increased awareness by the manufacturing and professional services sectors of their cyber exposures, while other segments that have historically been the clear leaders in terms of new Cyber buyers — such as healthcare, information technology, and financial institutions — become more mature.

Data breach still ahead

Data breach coverage, probably the best-known Cyber coverage due to U.S. notification laws and media attention, continues to be the coverage most sought after by buyers.

Following close behind is interest from buyers for coverages such as Cyber business interruption, Cyber extortion, funds transfer fraud, and system failure.

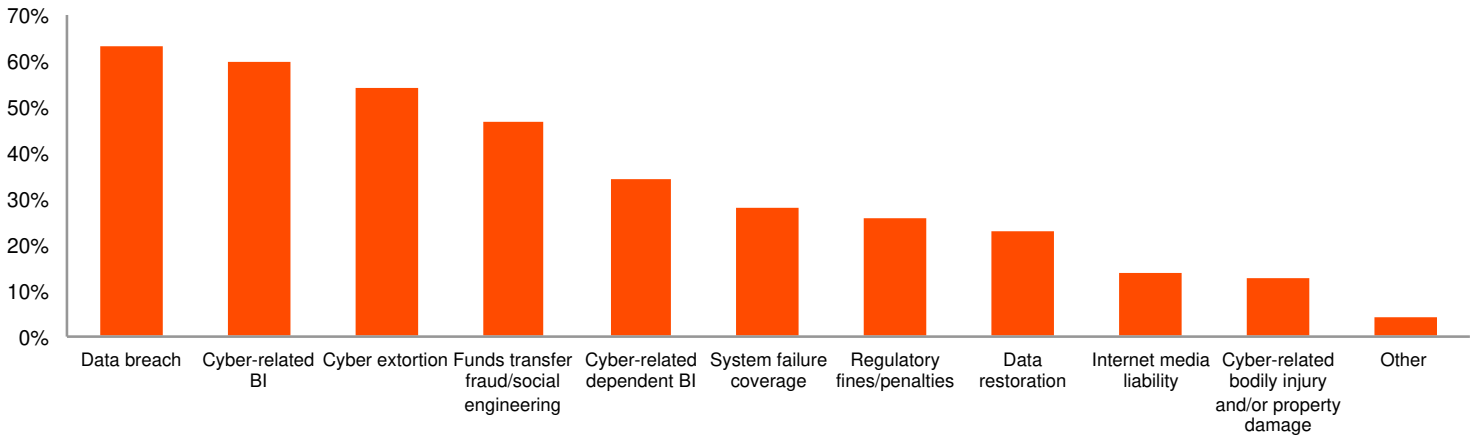
Funds transfer fraud, a form of social engineering fraud, involves deceiving someone to voluntarily transfer money. Due to increased awareness, it is not surprising that the survey responses indicate that interest in this type of coverage has increased. Whether it should be covered under a Cyber policy or a Crime policy is addressed later in this whitepaper.

This was the first of our surveys to include system failure coverage; a quarter of respondents noted their buyers having interest in it.

Cyber-related bodily injury and/or property damage do not rank highly as coverages that most buyers are interested in. This is also discussed in further detail later in this whitepaper.

A quarter of respondents noted buyers having interest in systems failure coverage.

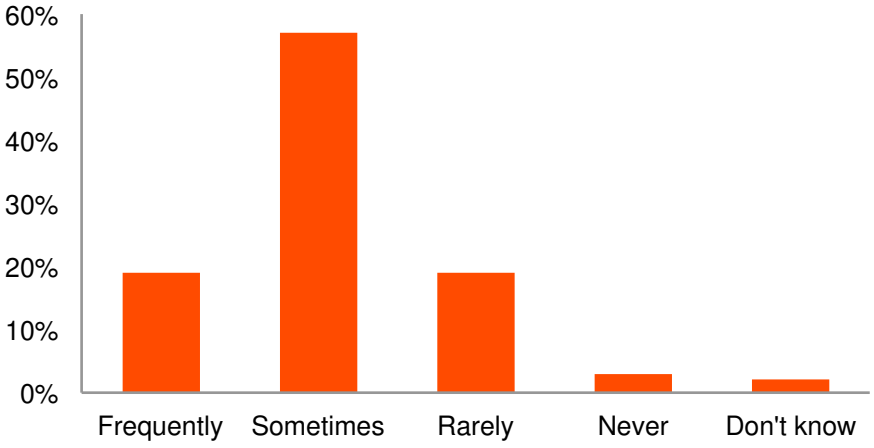
What Cyber coverages are NEW and RENEWAL buyers most interested in purchasing? (Please select top three)



Existing insureds seek higher coverage and limits

Consistent with previous years, almost two-thirds of respondents noted that their existing insureds were buying more coverages at renewal, with 76% reporting that renewal insureds “frequently” or “sometimes” also sought higher Cyber limits.

Are your renewal insureds requesting higher Cyber insurance limits?

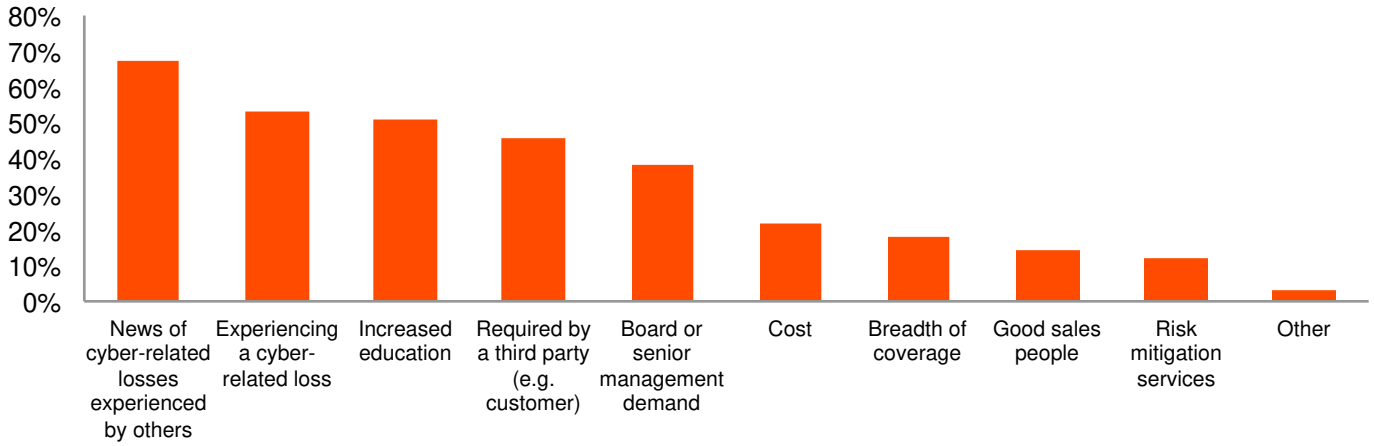


News of cyber losses impacts the decision to buy

While events like the Dyn DDoS and WannaCry ransomware attacks may not have had much impact on the underwriting and/or pricing of Cyber insurance, the survey indicates that they should have an impact on buyers and potential buyers of Cyber coverage.

As it has been every year, "news of cyber-related losses experienced by others" was the factor most often cited as a driver of the decision to purchase Cyber insurance. Increased education came in third, which supports what we see as the greatest obstacles to sales, discussed in the next section.

What do you see as the top driver(s) of Cyber product sales? (Choose up to three)



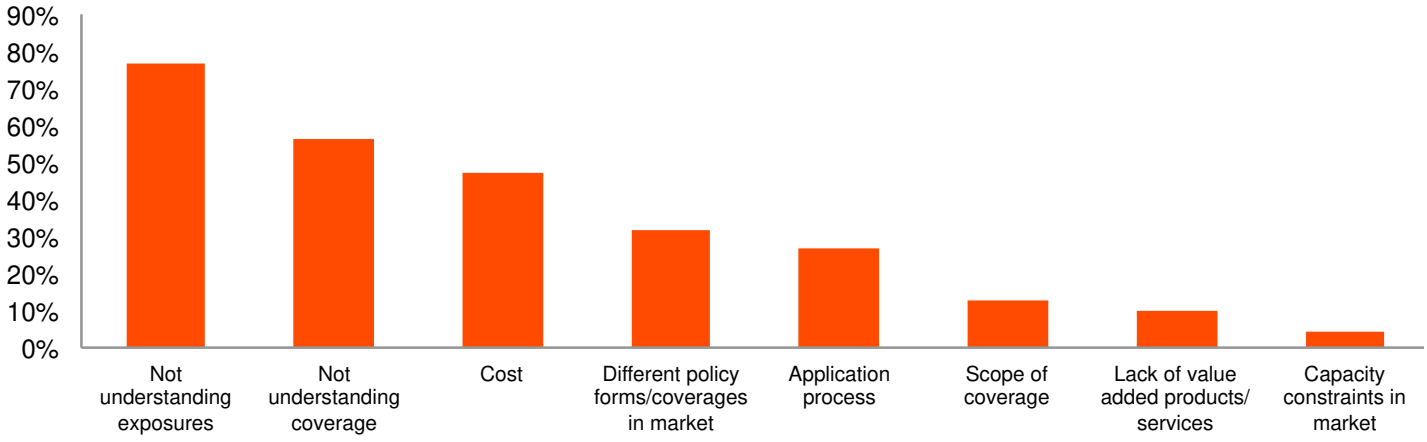
Not understanding the exposure still an obstacle to sales

According to 77% of the respondents, one of the biggest obstacles to sales is that potential buyers do not understand their exposures. Further, 56% of respondents also indicated that buyers do not understand the Cyber insurance coverages for those exposures. These top obstacles have remained constant year after year.

Top obstacles to sales have remained constant year after year.

Cost also figured prominently as an obstacle to selling Cyber coverage.

What are the biggest obstacles to writing/selling this coverage? (Select up to three)

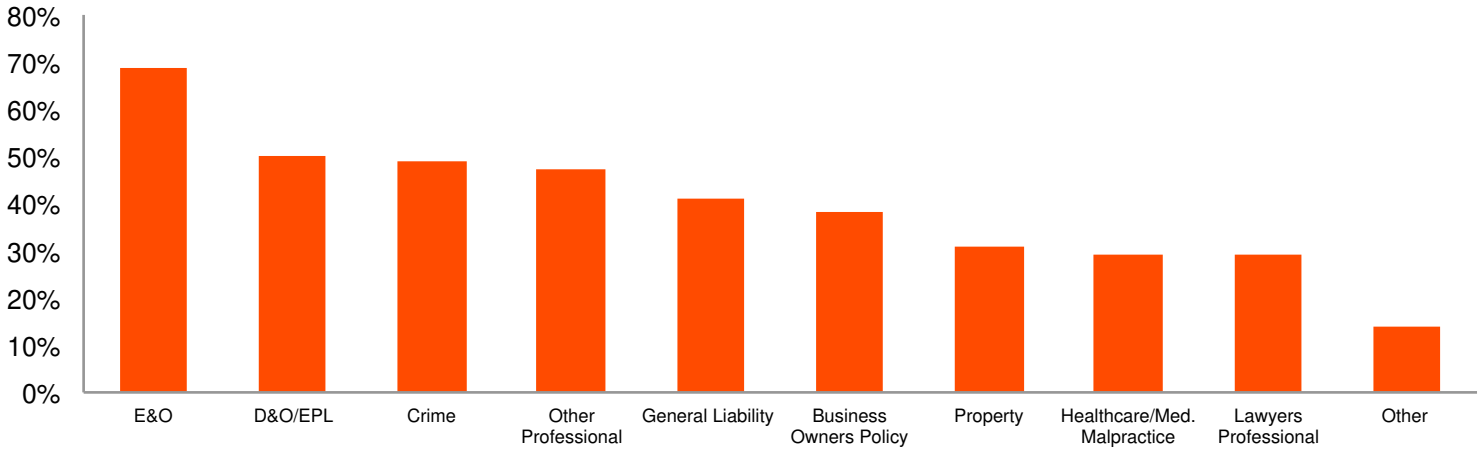


Endorsement to which policy?

Among the survey participants who indicated that they wrote or placed Cyber insurance coverage by endorsement, more than two-thirds (69%) indicated that they endorsed Cyber coverage onto Errors and Omissions (E&O) policies. All types of Professional Liability policies were also commonly endorsed.

The Crime policy is notably being endorsed more often than in previous years (in 2016 it was second to last on the list). This is possibly due to the social engineering exposure, which we cover a little later in this whitepaper.

If you write Cyber endorsements, what line(s)?

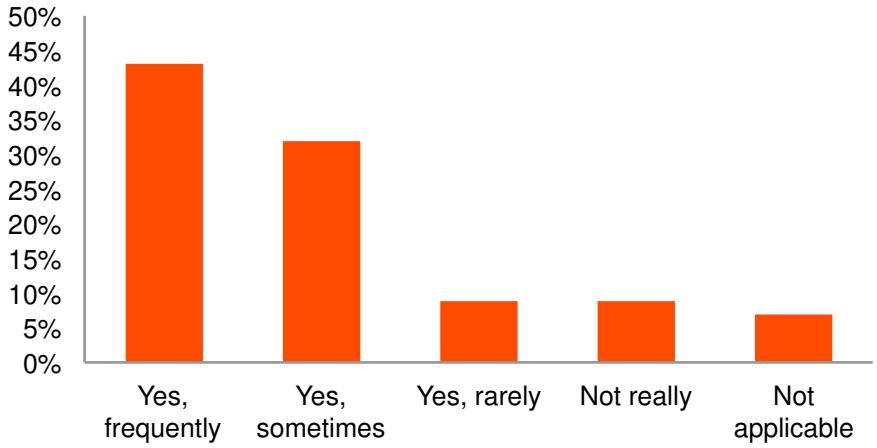


Clear shift from endorsement to stand-alone policies

When asked if a shift from Cyber insurance by endorsement to stand-alone policies had been observed, 84% of broker and underwriter respondents indicated "yes," with 43% of them indicating "yes, frequently."

This strong indication of a shift from endorsement to stand-alone policies suggests that endorsements may be a good way to introduce new customers to the product.

Have you seen Cyber business switch from endorsements to stand-alone policies?



Strong indication of buyers shifting from endorsements to stand-alone policies

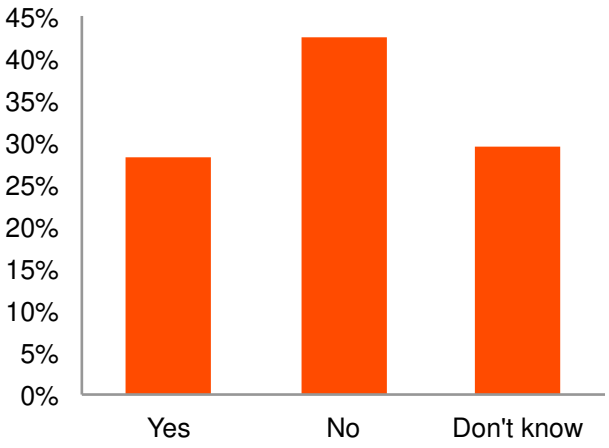
However, some feel that endorsements are not the right answer as they provide more restrictive coverage and that "the endorsements available tend to be insufficient in limit."

CLAIMS EXPERIENCE

Mixed feelings about claims handling

When brokers were asked if they noticed a difference in claims handling among carriers, about 28% indicated that they had. There were several comments on this topic indicating that some insurers were developing in-house Cyber claims units, as well as some comments on the use of vendors.

Have you noticed a difference in claims handling among carriers?



Generally we received diverse responses around claims handling:

"Standard markets seem to handle Cyber claims like they would any other professional liability loss, i.e. slowly and methodically. The specialty carriers and their retained vendors tend to provide service much more quickly and appropriately than the standard carriers - often on the same day [of a loss]."

"More of our carriers are adopting in-house breach response services to compete with each other. They are also offering some proactive risk management to help mitigate any future claims."

Claims handling by some carriers fell short of broker expectations:

"Some carriers are quick to pay all claims, as they are just getting started [in Cyber insurance], and some are more apt to look for language that gets them out of the claim."

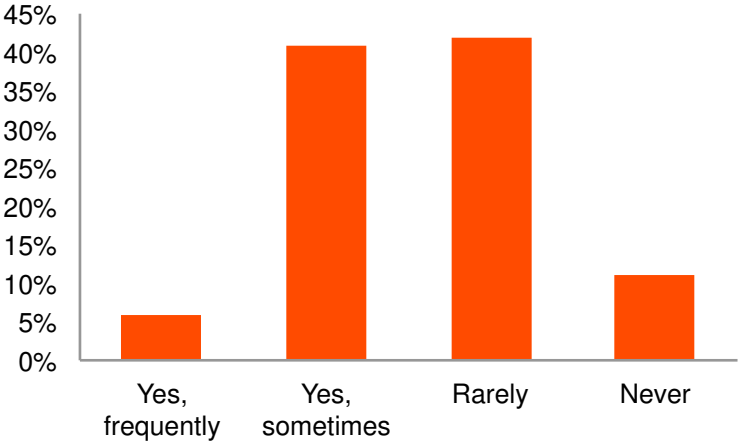
"There are only two or three really great claims handlers. Many use awful portals to hide their breach response information, which makes responding to an incident very cumbersome for a client."

BODILY INJURY, PROPERTY DAMAGE, AND SOCIAL ENGINEERING

Bodily injury and property damage still at low penetration

When asked whether insureds were inquiring more about cyber-related bodily injury and/or property damage (BI/PD) coverage, we noted a slight uptick in brokers and insurers who observed that insureds are asking "sometimes."

Are insureds inquiring about coverage for cyber-related bodily injury and/or property damage losses?



However, the interest in this coverage is still not widespread:

As noted earlier when we asked what coverages buyers were interested in most, cyber-related BI/PD came in last place. When we specifically asked whether insureds were inquiring about the coverage, over 50% noted it was "rarely" or "never". One broker commented that buyers ask about the coverage "only because they want an easy answer, not because they understand necessarily." We noted several brokers commented that they were proactively discussing or promoting this coverage to their insureds.

Brokers also noted that the coverage is available, although not widely offered.

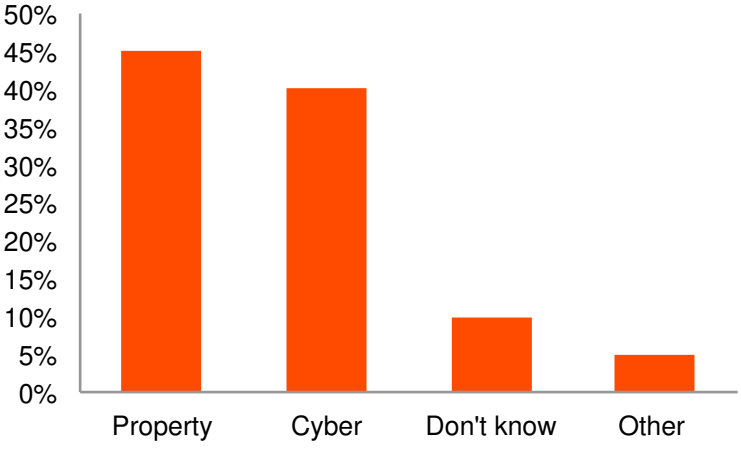
Brokers also noted that the coverage is available, although not widely offered. This is supported by the fact that about 34% of underwriters reported that they can provide cyber-related BI/PD coverage. That figure is about the same as last year. What has changed is that more underwriters (17%) indicated that they plan to add BI/PD coverage to their Cyber policies - last year only 9% said they planned to add the coverage.

Underwriters noted that "bodily injury and/or property damage losses are often covered within other lines" and "it's part of the Property policy and/or Liability, no need to be embedded to Cyber."

Policy 'home' of cyber-related property damage remains unsure

Almost 45% of respondents thought that cyber-related property damage would be better covered under a Property policy rather than a Cyber policy. However, 40% thought otherwise, and the comments indicated that consensus in the near future is unlikely.

Do you believe cyber-related property damage is better covered under a Cyber policy or a Property policy?



"Cyber-related property damage should ideally be covered under a Cyber policy, but the market needs to change in order to account for the risk."

In general, insurers were more likely than brokers to support keeping coverage for physical damage within a Property policy, e.g. "coverages should fall under the appropriate policy (e.g. Property, Liability, D&O etc.)."

"For the time being, all first-party losses for physical damage should still be covered under a Property policy. However, physical damage arising from cyber causes should soon be shifted onto Cyber policies since the risks of property damage caused by cyber can be better understood by Cyber markets."

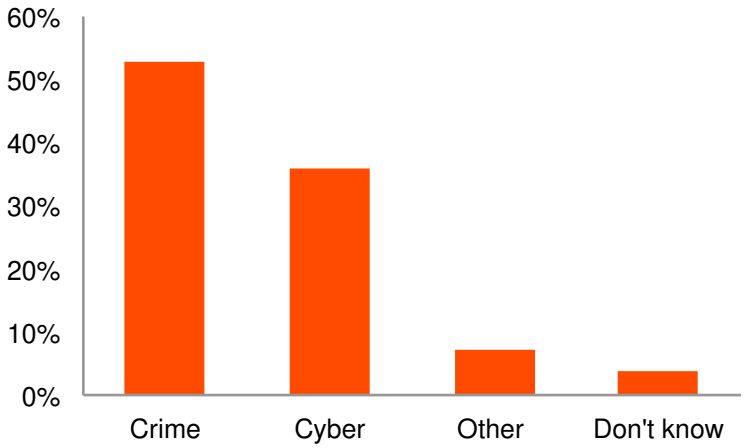
"Cyber-related property damage should ideally be covered under a Cyber policy, but the market needs to change in order to account for the risk."

Funds transfer fraud – preferred 'home' is the Crime policy

Social engineering, or funds transfer fraud coverage, has become a greater concern for insureds, this year ranking fourth as coverage that buyers are most interested in purchasing. With this rise in interest and the availability of coverage, we asked brokers and underwriters if funds transfer fraud would be better covered under a Cyber or Crime policy.

The majority felt that the coverage should be provided under the Crime policy. Interestingly, the divide was relatively narrow among brokers (45% Crime; 40% Cyber) and more divergent among underwriters (70% thought that cyber-fraud losses should be covered under a Crime policy).

Do you believe funds transfer fraud loss due to social engineering fraud is better covered by a Cyber policy or a Crime policy?



The majority of respondents felt that funds transfer fraud coverage should be covered by the Crime policy, though this was largely driven by underwriter responses

The range of comments received on this topic indicated uncertainty regarding how best to incorporate coverage for cyber-related losses into the established categories of insurance:

"By and large, I'll say Crime [policy] for fraud losses, but for some risks, buying coverage on a Cyber policy makes sense."

"[Stolen] funds are better [covered] under a Crime policy, but if it's data, it is better [covered] under a Cyber policy."

"It's a misnomer to suggest that a fraud conducted online was a "Cyber" loss - the argument can be made [that coverage] is better suited to Cyber. At the very least we advocate trying to buy the two coverages from the same carrier."

"I would like to see Cyber [coverage] integrated into Property, [Electronic Data Processing], and General Liability forms. Just as equipment breakdown was added as an additional cause of [Property] loss, so too Cyber (or parts of it) could be added to existing forms with ease."

"It would make it much easier to introduce and integrate Cyber coverages to the average commercial insurance buyer. Having to help a client understand that they need an entirely new line of [insurance with] as many as five different types of coverage is a much more difficult sale."

INTERNATIONAL MARKETPLACE

As the product evolves and privacy laws start taking effect in other countries, we expect the reach of this product to expand geographically.

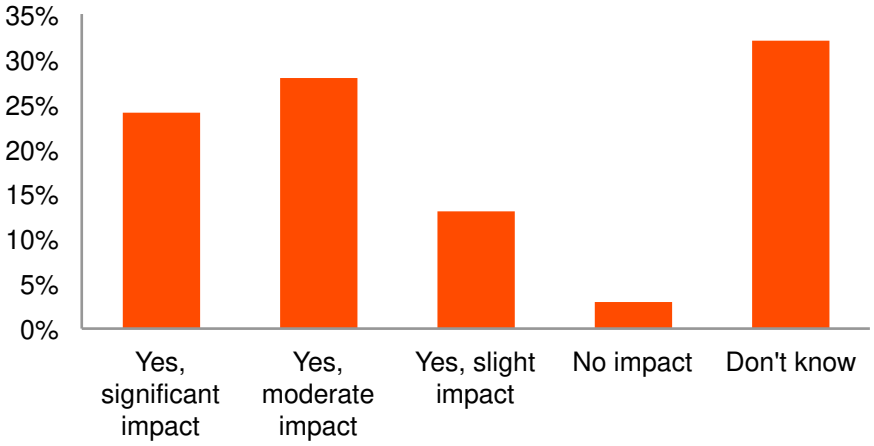
It's not just about the U.S.

This year respondents were asked if they were located in the U.S., U.K./Europe, or elsewhere. Over 25% of respondents were located outside the U.S. We also asked what percentage of respondents' business was based in the U.S., and we noted that 24% place less than half their business in the U.S.

GDPR impact undecided

Participants were asked whether they thought there would be a significant impact on the take up rate for Cyber insurance when the European Union's updated General Data Protection Regulation (GDPR) takes effect in May 2018. Slightly more than half of respondents thought that it would have a significant or moderate impact; the rest thought there would be little or no impact, or didn't know.

Do you think EU cyber regulations will have an impact on Cyber insurance take up in Europe?



FINAL COMMENTS

Overall, some way to go to meet all needs

Every year, the survey asks participants the fundamental question: "Do you think that Cyber insurance policies are meeting the needs of insureds?" This year, 82% said "yes, sometimes" and 15% said "yes, always."

General comments on the state of the Cyber insurance market:

"There needs to be a shift in thinking about Cyber liability coverage across the marketplace. Treating the coverage as a service rather than a typical insurance policy will allow people to better utilize the value-added services available, thereby creating a stronger relationship and desire for coverage. If the change in mindset can occur, I believe insureds would be more apt to see the coverage as a means of complementing their IT systems and security. Cyber exposure is not a risk that can be [eliminated] or transferred. It needs to be managed through a comprehensive risk management program that includes security, training, and insurance."

"We need to be able to sell a product that varies from carrier to carrier based on a client's specific exposures."

"The cyber risk is evolving and becoming more complex. Meanwhile many new insurance carriers come in this area and unfortunately their underwriters are not really ready."

In summary, the market is expanding as cyber events keep making headline news, existing insureds look to buy more coverages, increase their limits, and move from endorsements to stand-alone policies. Regulation should also drive sales in those countries where notification laws are put in place. Hindering growth continues to be the non-standardization of policy forms and a persistent lack of understanding of cyber exposures and insurance coverages. At this time, there is no consensus as to where other cyber-related losses will be covered, such as bodily injury, property damage, or funds transfer fraud. For now, the Cyber insurance product is meeting needs of insureds most of the time.

"The cyber risk is evolving and becoming more complex. Meanwhile many new insurance carriers come in this area and unfortunately their underwriters are not really ready."

ABOUT PARTNERRE

PartnerRe is a privately-owned, pure-play global reinsurer with a strong balance sheet and the scale and expertise to meet our clients' needs across lines and markets. Relationships are central to our business. We give our clients our undivided focus to deliver both standardized and innovative customized solutions.

How can PartnerRe help you?

Come to us for customized reinsurance solutions for all types of cyber risk.

Look to us for the latest information on Cyber developments and challenges, through our hosted events, conference attendances and this annual Survey of Cyber Insurance Market Trends, carried out in partnership with Advisen Ltd.

Contact us to discuss Cyber risk solutions or to find out more about this survey: https://partnerre.com/risk-solutions/cyber-risk/

Your contacts

Catherine Rudow
Cyber P&C North America
catherine.rudow@partnerre.com
+1 203 485 8082

Christopher McEvoy
Cyber P&C Europe
christopher.mcevoy@partnerre.com
+41 44 385 37 98

Markus Bassler
Cyber Specialty Property
markus.bassler@partnerre.com
+41 44 385 34 48