Advisen
Transforming • Insurance℠

PartnerRe

# Cyber Insurance – The Market's View.

## PartnerRe & Advisen

For the sixth 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.

## Survey Information

This global survey was carried out during the third quarter of 2019.

271 brokers and 96 underwriters – all involved in cyber insurance - shared with us their observations and views of the cyber insurance marketplace. 71% of respondents were located in North America, 21% in the United Kingdom (UK) & Europe, 4% in the Asia/Pacific region, with the remainder located in Bermuda, Latin America, the Middle East and Africa. North America, the UK & Europe and the Asia/Pacific region also topped the list of regions in which at least 10% of the respondents' insureds are located.

We sincerely thank all respondents for their time and insights. These findings and thoughtful responses help bring to light many interesting facets of a rapidly evolving, essential and fascinating segment of the insurance industry.

This report summarizes the survey's key findings. However, we received many more valuable insights than could be incorporated in this report. If you would like more information, or to request to reproduce material herein, please contact the Editor. To discuss cyber risk solutions, please contact PartnerRe's cyber experts (see contact details at the end of this report).

# Key Survey Findings

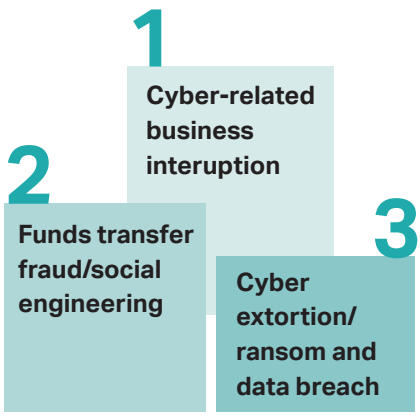
## Sales motivations

- Professional services and manufacturing/industrials both increased their presence in new cyber sales, knocking healthcare off the top spot.
- Losses continue to drive sales. The top driver of new and increased cyber sales was "news of cyber-related losses experienced by others".
- "Not understanding exposures", "not understanding coverage" and "cost" remain the top three obstacles to writing and selling cyber insurance.
- GDPR impact will remain uncertain until there's resolution on the insurability of GDPR fines.


**Top driver of new/increased sales is:** "News of cyber-related losses experienced by others"

## Coverage requests

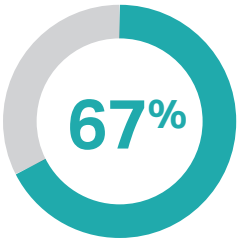
- The switch from endorsement to standalone continues. Wanting higher and dedicated cyber limits and expanded coverage were the main reasons for switching. The indication is that, despite the fact that lack of exposure and coverage understanding is still the primary obstacle to cyber sales, once on cover, insureds are gaining a better understanding of their exposure.
- The most-requested cyber coverage types were notably similar to last year: 61% of respondents included "cyber-related business interruption" as one of their top three choices. This was closely followed by "funds transfer fraud/social engineering" (58%), "cyber extortion/ransom" and "data breach" (both at 56%).
- Renewal insureds of cyber insurance are "frequently" (21%) and "sometimes" (66%) requesting higher limits, again indicating an improving appreciation of cyber exposures.




**Most-requested coverage types**

## Policy overlaps and unsettled areas

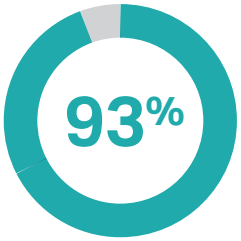
- There's been a slowdown in policy overlap: Last year, 51% noted an increase in overlap, but in this year's survey only 36% noted an increase.
- 67% of underwriters reported that they are worried by the presence of non-affirmative/silent cyber coverage in specialty property risks.
- The majority of underwriters and brokers agreed that funds transfer fraud loss/ social engineering should be covered on the crime, not the cyber, policy; underwriters were clearer on this (74%) than brokers (52%).
- When asked if cyber-related bodily injury and/or physical damage should be covered by a dedicated cyber or the property policy, the majority of underwriters opted for the property policy (54%), while the majority of brokers opted for the cyber policy (49%).




**of underwriters are worried by non-affirmative cover in specialty property risks**

## Risk aggregation

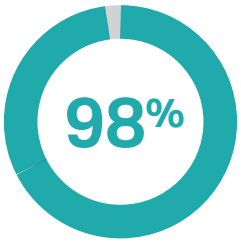
- 93% of underwriters said that they analyze the systemic nature of the cyber exposure.
- 45% actively manage aggregation in-house, 29% do this in house with outside vendors (an increase on last year), many others are moving towards actively managing aggregation.
- 35% said that aggregation management "always" impacts their underwriting or pricing decisions, 38% said "sometimes", and only 15% said "no". Results suggests a progressive integration of aggregation management into cyber risk underwriting.




**Analyze the systemic nature of the cyber exposure**

## Overall market view

- The market is much more competitive than last year (91 % of underwriters and 84% of brokers agreed), and this is true of both large and small accounts.
- 66% of brokers felt that coverage expansion is necessary to attract new insureds; 49% of underwriters agreed.
- Brokers reported that cyber insurance pricing (61% agreed) and coverage (72% agreed) are becoming more consistent among carriers.
- Despite improvements, consistency is still a concern to brokers and the majority (69%) continue to limit the number of carriers that they place business with.
- Survey respondents reported that, overall, cyber insurance meets (58%) or partly meets (40%) the needs of insureds.

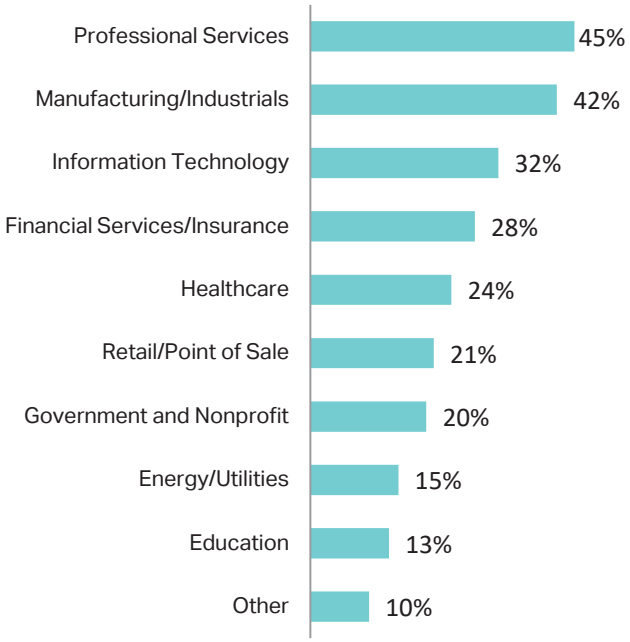



**Agreed that cyber insurance meets or partly meets the needs of insureds**

# Sales motivations

## Who's new to the market?

**Q** What industries brought the most new to market buyers of cyber insurance? Please select top three:




Long gone are the days when the perception was that retail organizations had the highest exposure to data breach. Indeed in last year's survey it was "healthcare" that took the top spot (42% noted this as one of their top three new buyer segments), while "retail/point of sale" only featured in the top three of 24% of survey respondents.

This year, we looked separately at new buyers for cyber standalone and endorsement, and interestingly noted no significant variation: "Manufacturing/industrials", "professional services" and "information technology" took the top three places for both policy types. "Healthcare" not only moved off the top spot, but also out of the top three.

## Losses still main sales driver

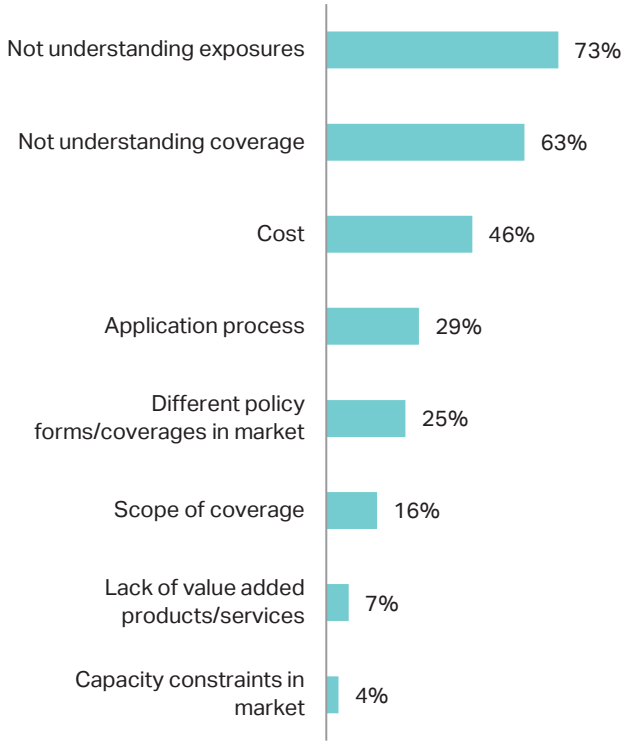
**Q** What do you see as the top driver/s of new/increased cyber insurance sales? Please select top three:


The top drivers of new and increased cyber sales followed a similar pattern to last year, but the number one driver, "news of cyber-related losses experienced by others", increased its lead; 68% of respondents put this in their top three compared to 56% in 2018. "Experiencing a cyber-related loss" came in second at 54%. One broker commented, "Getting a large organization to buy a new line of insurance is always a challenge. Getting the board to approve the new expense, even if they understand the exposure and the risk that faces their organization is never easy unless they have experienced a loss."

## Obstacles to sales

According to the survey, "not understanding exposures" (73%), "not understanding coverage" (63%) and "cost" (46%) remain the top three identified obstacles to writing and selling cyber insurance. That cost is still a major obstacle to sales is no surprise given the other two leading categories.

**Q** **What are the biggest obstacles to writing/selling cyber insurance? Please select top three:**




We received a lot of additional comments to this question. One underwriter noted for cost that "Premiums are already very low while the market doesn't clearly know how high or low the long-term loss ratio will be. There's simply a lack of historic data."

Broker comments included several of a similar nature to the following: "If they use an outside IT company, clients believe that is sufficient for that company to have cyber coverage"; the feeling that "we have good systems in place, we won't get hacked"; and "pride of IT person", "reliance on IT security". On the positive side, several noted that "once converted [new insureds] are 'true believers'" and that "once [insureds] understand the exposures and coverages they usually see the value, and the cost for $5 million - $10 million in limits seems reasonable. However, getting them to understand is difficult."

One broker noted that misinformation around claims is causing some to be skeptical: "rampant circulation of bad information. For example, news stories that seek to 'expose' cyber insurance and not paying claims, when in fact, the claims are being brought under non-cyber policies. Those articles, properly written, would encourage companies to purchase specific cyber insurance instead of relying on 'silent cyber' to protect them." More information on losses and scenarios affecting similar organizations could help here, survey respondents suggested.

## Uncertain impact of GDPR

In a question devoted to the impact of the European Union's General Data Protection Regulation (GDPR), both underwriters and brokers agreed that it has affected the demand for cyber coverage (respectively 82 % and 70 % agreed). One respondent noted, "GDPR, and its second cousin CCPA in California, raised the level of awareness and helped promote education for the need for cyber coverage."

Over three-quarters of both brokers and underwriters, however, felt that the effect of GDPR on cyber insurance will continue to be muted until there are additional "headline losses" and legal precedent. When asked whether GDPR will lead to first-party claims losses higher than in the U.S., one respondent noted, "Entirely dependent on the insurability of GDPR fines. Legal precedent must be set per member state before anyone can make a call on this."

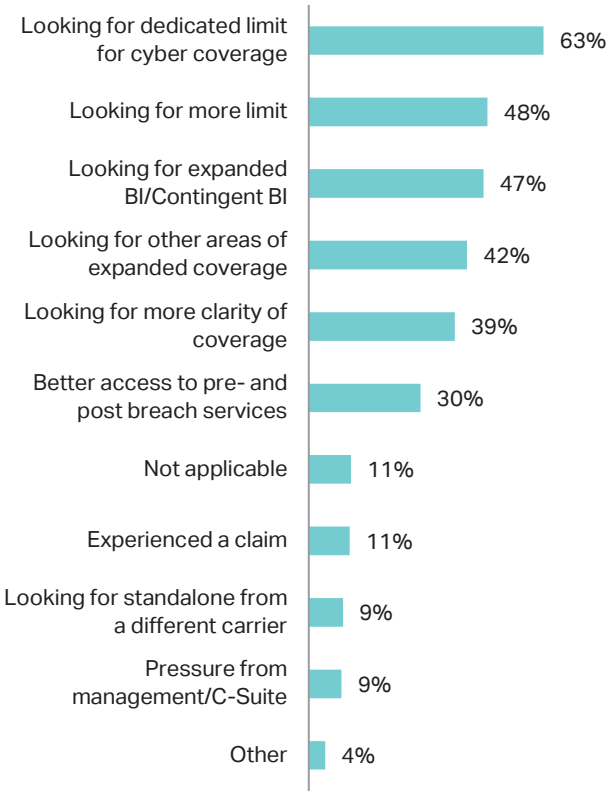
# Coverage requests

## The switch from endorsement to standalone continues

The survey results revealed that errors and omissions and professional indemnity remain the most commonly endorsed policies for cyber (63% of all respondents included these policies in their selection), followed by small commercial/package, directors & officers/ employment practices liability, crime and general liability policies.

However, most respondents reported having seen insureds switch from endorsement to standalone cyber, so the trend that we reported on last year clearly continues.

**Q** If you have seen cyber business switch from endorsement to standalone policies in 2019, what is the main reason/s? Please select top three:




Underwriters and brokers both found that buyers primarily make the move from endorsement to standalone for reasons of limits and coverage. This suggests - despite the fact that "not understanding exposure" is still the primary obstacle to cyber sales - that once on cover, insureds are gaining a better understanding of their cyber exposure.

Looking for "dedicated limit for cyber coverage" topped the bill with 63% of respondents noting this as one of the key reasons for switching to standalone, closely followed by "more limits" and "expanded business interruption/contingent business interruption" (both at ca. 47%), "other areas of expanded coverage" (42%) and "more clarity of coverage" (39%). "Better access to pre- and post-breach services" followed at 30%.

> "This suggests – despite the fact that "not understanding exposure" is still the primary obstacle to cyber sales – that once on cover, insureds are gaining a better understanding of their cyber exposure."

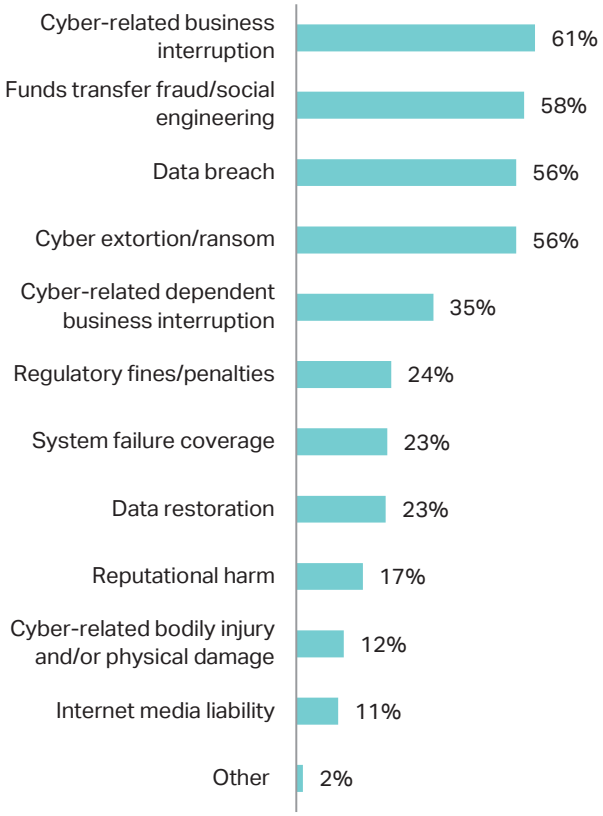
One broker respondent linked switching to the fact that agents "are becoming more comfortable with selling the [cyber standalone] product". Other cited reasons included "avoiding non-cyber related exclusions" and several respondents referred to "contractual requirements".

It's interesting that losses lead the driver table for new and increased cyber sales, but that any subsequent switching from endorsement to standalone is primarily in response to limits and coverage (through an improved appreciation of own exposures).

## Most requested coverage types

With the indication that insureds are better understanding their cyber exposures, the survey results on which coverages buyers are most interested in purchasing sheds light on the cyber events that most concern them.

**Q** What coverages are (new and renewal) buyers most interested in purchasing? Please select top three:




The top four survey results were notably similar to last year, revealing an ongoing and strong interest in guarding against business interruption losses; 61% included "cyber-related business interruption" as one of their top three choices. This was closely followed by "funds transfer fraud/social engineering" (58%), "cyber extortion/ransom" and "data breach" (both at 56%). Although we present the combined results for underwriters and brokers, the percentage of underwriters that put "funds transfer fraud/social engineering" as a top three buyer interest category was a notable 11 points higher than that of brokers.

## Upward limits

In line with buyers having a better appreciation of exposures and switching from endorsements to standalone for dedicated cyber limits and higher limits, both underwriters and brokers reported that renewal insureds of cyber insurance are "frequently" (21%) and "sometimes" (66%) requesting higher limits. Only 11% reported that they have observed no interest in higher limits at renewal.

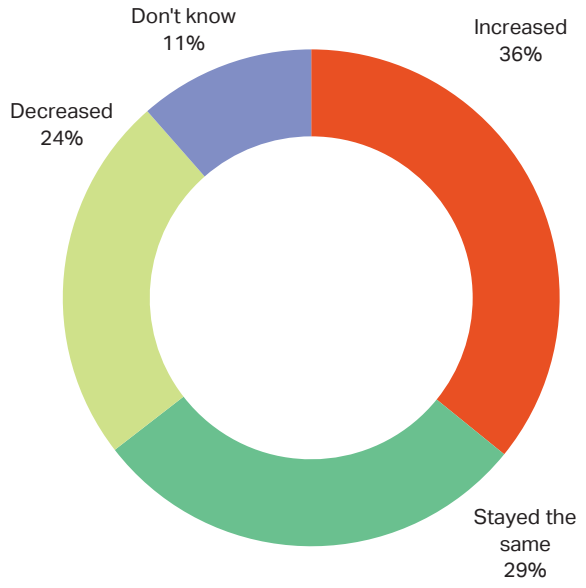
# Policy overlaps and unsettled areas

## Policy overlaps

This year's survey indicates that the overlap between cyber and other policies continues to worry the industry.

Comments noted that overlaps most often occur with property, crime, and kidnap and ransom policies. Brokers reported that they see coverage on traditional lines being broadened in some cases to provide affirmative coverage for cyber risk.

**Q** Coverage overlap between cyber and other policies has:



On a positive note, we observed an improvement compared to last year: 51% noted an increase in overlap last year, but in this year's survey only 36% noted an increase. 24% of this year's respondents reported a decrease in overlap and 29% said that overlap had stayed the same. One respondent added, "As more people move to standalone cyber policies there is starting to be clear delineation of which policy picks up which exposure." Another reported, "There is a large overlap, however, as claims increase I feel cyber will be stripped out of non-cyber policies as they aren't getting proper premium for their exposure."

## Non-affirmative cyber

67 % of underwriters reported that they are worried by the presence of non-affirmative/silent cyber coverage in specialty property risks. One respondent noted, "Concerned but realistic. Clarity in coverage is important to reduce uncertainty. We do not live in a perfect world. In this imperfect world, multiple insurance policies will have to come into play after a single event, such as property coverage also responding after a cyber event. The beast of 'silent cyber' is here to stay."

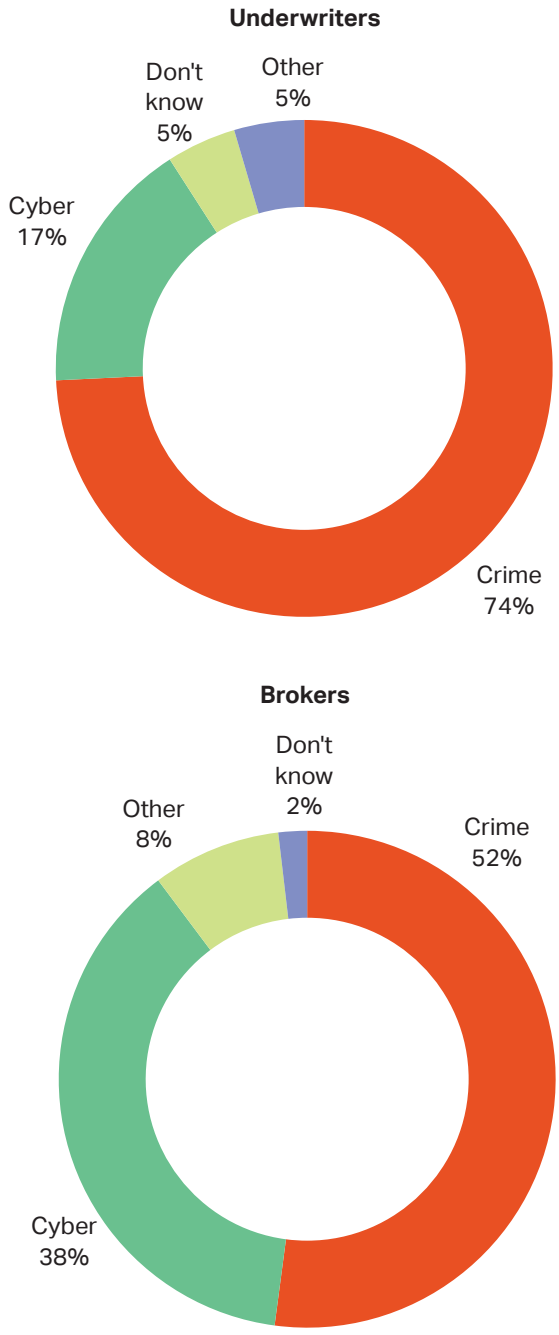
## The crime vs. cyber question

With funds transfer fraud loss/ social engineering so high on the list of coverage types that new and renewal buyers are most requesting, the survey results on where this should be covered (on the crime or cyber policy) are of great interest.

Crime was the preference of both underwriters and brokers, but underwriters were much clearer on this (74%) than brokers (52%). One underwriter noted, "Cyber for SMEs, crime for large enterprises". Brokers had a lot of comments here: "If cyber is the trigger then it should fall under a cyber policy"; "I'm generally in favor of using cyber policies for IT related losses until such time as traditional crime policies are more robust and 'cyberized'"; "I consider social engineering a cyber breach, so dancing between a cyber and crime policy gets complicated when it shouldn't be." Other brokers suggested a blended solution could work better: "Cyber and crime can be impacted at the same time. As electronic fraud is increasing, I would say that now more than ever combined policies are desirable."

Other brokers indicated that they don't have a strong opinion on this as long as there is coverage somewhere and the distinction is clear.

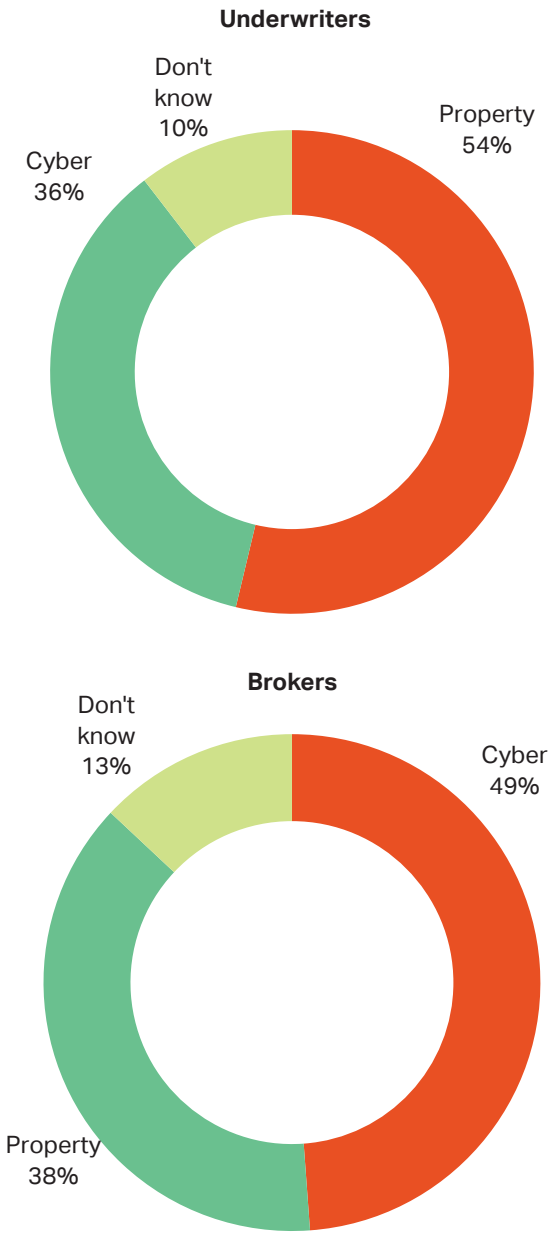
**Q** **Where do you believe funds transfer fraud loss due to social engineering should be covered?**



## Where to put cyber-related bodily injury and physical damage?

47% of underwriters and 45% of brokers reported that they frequently or sometimes receive requests for cyber-related bodily injury and/or physical damage coverage. So the question of whether this should be covered under a dedicated cyber cover or a property policy is significant.

**Q** Do you believe cyber-related physical damage should be covered under a dedicated cyber cover or property policy?




There was once again a split in views between underwriters and brokers. The majority of underwriters opted for the property policy, while the majority of brokers opted for the cyber policy. Comments, however, showed ongoing differences of opinion.

One underwriter noted, "If the physical damage was caused by a cyber incident then I believe a cyber policy should respond". Another commented, "This is an ongoing debate in our company. As a former property underwriter gone cyber underwriter, I am convinced that it should be covered under a property policy…. but there is no doubt that the underwriting process must include cyber risk competence, which also holds true for almost all LoBs going forward."

In response to the same question, one underwriter noted that there is "not enough premium in cyber market for property damage", a sentiment echoed by another who commented, "But then not at a price like we see in the market now. Pricing of cyber insurances are way too low compared to the risk we are taking".

One broker noted, "I like that I am seeing it sub-limited under cyber policies. I do think that if insureds aren't careful, a cyber-related physical damage claim could eat up the limits better used for a traditionally covered cyber claim."

When asked if their company's cyber insurance provides coverage for cyber-related bodily injury and/or physical damage losses, 62% of underwriters reported that it does not. One underwriter stated that they consider this, but only "on a case by case basis".

# Risk aggregation

## Positive trends

As dedicated and higher cyber limits are sought, and given ongoing issues including policy overlaps and non-affirmative coverage, we asked underwriters about how they manage cyber risk aggregation, whether aggregation management impacts their underwriting or pricing decisions, and if they analyze the systemic nature of the exposure; to the systemic question we received a resounding "yes" (93%).

As to whether companies are actively managing risk aggregation: 45% do this all in-house, 29% do it in-house with outside vendors, and the majority of the remainder are moving in the direction of actively managing cyber risk aggregation. Interestingly, compared to last year, the use of outside vendors gained some ground from "all in-house".

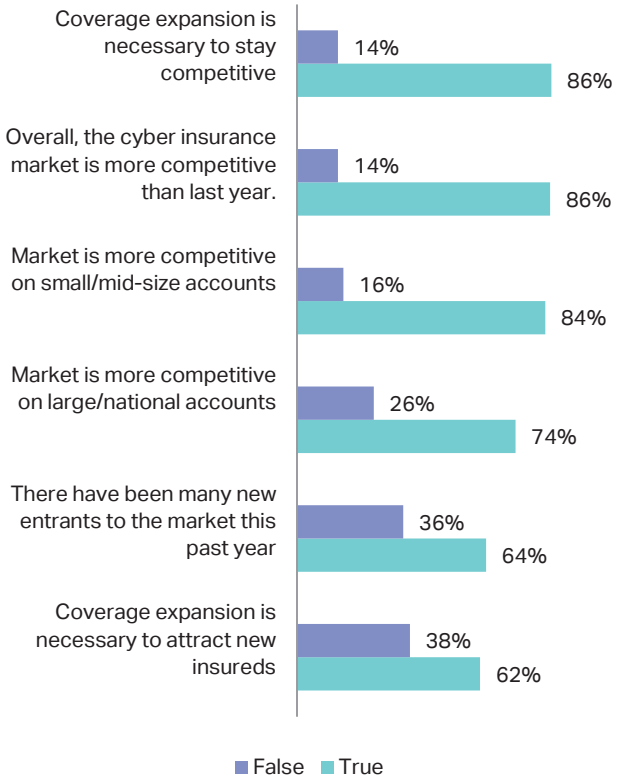
When asked if aggregation management impacts their underwriting or pricing decisions, 35% said "always", 38% said "sometimes" and only 15% said "no". Compared to last year, the (6 percentage point) increase in "always" matches the decrease in "sometimes", suggesting a progressive integration of aggregation management into cyber risk underwriting. A few respondents commented that aggregation management governs their use of large limits or prompts them to decline high-risk accounts.

In contrast, most underwriters (41%) do not rely on vendors to evaluate the third-party relationships of their insureds (37% did not know). This question elicited a range of comments all questioning the usefulness of vendors to help monitor third-party risk; for example, "No third party tools currently offer good enough services that can be relied upon for underwriting."

# Overall market view

## An increasingly competitive market

**Q** Please answer true or false to the following:




**Combined Results**

We asked about the competitiveness of the market and heard loud and clear that the market is much more competitive this year compared to last year (91 % of underwriters and 84% of brokers agreed), and that this is true for both large and small accounts.

Underwriters expressed concern about the continued downward pressure on prices: "Care needs to be taken that the cyber market remains sustainable. We never faced a real systemic event affecting a large quantity of insureds. Further, coverage broadened tremendously and the industry needs to make sure to understand exposures and get underwriting and pricing right." Another cited a "price war" occurring as brokers shop their business around seeking the lowest quotes. Another referred to "Very competitive pricing

and T&C's. Soft market for no clear reason other than everyone wanting a piece of the pie."

While opinions were similar across the market in terms of competitiveness, differences in opinion arose between underwriters and brokers as to whether coverage expansion is needed to attract new insureds; 66% of brokers felt that coverage expansion is necessary, only 49% of underwriters agreed.

## Market consistency continues to improve

Broker respondents reported that cyber insurance pricing (61% agreed) and coverage (72% agreed) are becoming more consistent among carriers, in general or in some respects. These results are the highest indication of consistency that the survey has seen so far.

However not all respondents agreed: "Policies among carriers are still very different – so pricing is different"; "Cyber is the least consistent and most troubling thing to compare between carriers. Expert knowledge is required to properly understand the coverages and what they are intending to cover. Just because they have the same coverage title does not mean they cover the same exposure"; "Full reviews must be done on each [policy] to compare apples to apples for coverage."

Timing seems to be key. Respondents noted: "There are a few market leaders, the rest tend to adopt those market leaders' coverage terms lagging a year or two behind"; "Policy language has not standardized at all even for insuring agreements that have been around for years. New innovative coverages are being introduced to the market frequently. One carrier leads the charge and then the rest follow in order to remain competitive."

The soft market received a lot of comments: "New markets are sometimes underwriting aggressively to grow their share"; "The market has remained extremely soft and profitable for carriers. 30-40% savings and multiple coverage enhancements on a renewal when the program is marketed properly is not uncommon". Another noted a distinction, "New carriers entering the market along with insurtech companies are keeping the price down. However, carriers that write a lot of excess in higher towers, and carriers that write larger/more complex risks are slightly hardening their prices."

Given that consistency remains a concern to brokers, it is not surprising that the majority of brokers (69%) still limit the number of carriers that they place business with.

Differences in claims handling were reported by 44% of brokers. Responses revealed that brokers have experienced and expect differences in carrier claims handling; "There certainly is a difference. This isn't to say that newer cyber markets are unable to handle claims, but when dealing with larger and more complex clients it is important to make sure they have strong claims handling on primary"; "There are several new carriers out there who don't have the infrastructure or people to be good at the claims process yet". Many noted that they have not yet had a claim.

## Overall satisfaction is high

So are cyber insurance policies meeting the needs of insureds? We posed this question to the market and respondents almost all agreed that cyber insurance does meet (58%) or at least partly meets (40%) the needs of insureds. Many respondents highlighted the need for more education on the exposure, coverage and risk management steps that can be taken. Others emphasized the need to coordinate coverages across programs to ensure the most effective response and for constant vigilance in keeping policy wordings reflective of current exposures.

And from a purely practical stance, one respondent noted, "I know not having cyber policies doesn't meet the insured's needs, so having one is better than not."

Another offered a thought that encapsulated many of the views shared in the survey: "Cyber insurance is a robust marketplace that constantly attracts new service providers and new buyers. Because the landscape is constantly changing and vibrant, it is intellectually appealing to many of us. But that complexity can make cyber insurance intimidating to new buyers, which shows the importance of education and outreach. You can't 'scare' customers into buying this insurance (and scare tactics are tacky). Thoughtful education, and knowledge that accumulates over time and builds true depth of understanding, serve to develop good cyber buyers/policyholders."

# 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 virtually all markets, risks, lines and products. Relationships are central to our business. We give our clients our undivided focus to deliver both standardized and innovative customized reinsurance solutions.**

## How can we 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.

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

## Your contacts

**Andrew Laing**
Cyber P&C Worldwide
andrew.laing@partnerre.com
+1 203 485 8438

**Ho-Tay Ma**
Cyber P&C North America
ho-tay.ma@partnerre.com
+1 203 485 4348

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

**Editor:** Dr. Sara Thomas, PartnerRe;
sara.thomas@partnerre.com

## Disclaimer:

The information contained in this document has been developed from sources believed to be reliable. However, the accuracy and correctness of such materials and information has not been verified. We make no warranties either expressed or implied nor accept any legal responsibility for the correctness or completeness of this material. This information should not be construed as business, risk management, or legal advice or legal opinion. Compliance with any of the recommendations contained herein in no way guarantees the fulfillment of your obligations as may be required by any local, state or federal laws. Advisen assumes no responsibility for the discovery and/or elimination of relevant conditions on your property or at your facility.