Advisen
A ZYWAVE COMPANY

PartnerRe

Cyber Insurance

The Market's View

Survey Information

Christopher McEvoy

Cyber Worldwide
christopher.mcevoy@partnerre.com

Ho-Tay Ma

Cyber North America
ho-tay.ma@partnerre.com

Georgina Lee

Cyber Asia Pacific
georgina.lee@partnerre.com

A global cyber survey by PartnerRe and Advisen, now in its eighth year.

264 cyber insurance brokers/agents and 112 cyber underwriters took part.

We sincerely thank all respondents for their valuable time and insights.

PartnerRe is a leading multi-line global reinsurer with a strong balance sheet and cyber risk expertise. We look forward to hearing from you about the survey findings and/or to discuss your cyber needs.

For more on our cyber risk solutions:
partnerre.com/risk-solutions/cyber-risk

Key Survey Findings

"As many in the market will have observed from own experience and headlines, the frequency of extortion/ransom losses has increased. Result, the cyber market has hardened. With headline events reported as being far and away the main driver of cyber sales, it's no surprise that higher limits are being sought and extortion/ransom has overtaken cyber-related business interruption as the most requested coverage. The survey also clearly identified that underwriting has become more disciplined - risk scanning is now firmly embedded in underwriting, more focus is being put on analyzing and modelling systemic exposures, and the majority of underwriters are looking at solutions for extortion/ransom with coinsurance of the buyer. Insureds are now having to work a lot harder to demonstrate improved security to secure coverage.

"Looking forward, coverage evolution, particularly the refining of extortion coverage, will be important for the product to remain viable, especially in the US and Europe. These and many more market insights can be found in the following slides."

Christopher McEvoy
Head of Global Cyber Risk, PartnerRe

Cyber extortion/ransom overtakes "Cyber-related business interuption" as the coverage that buyers are most interested in – 86% put this in their top-3.

"News of cyber-related losses" increases its lead (+14 percentage points) as the **top new/increased cyber sales driver.**

Underwriters are cautious about covering extortion demands (where legally insurable) - 23% prefer exclusion (c.f. only 6% of brokers) and almost half opt for inclusion with coinsurance of the buyer.

"Cost" continues its rise up the ranks as a major sales obstacle – now in 2nd place, after 1st place "Not understanding exposures".

Risk scanning is firmly established in underwriting – 65% do this already and a further 23% are looking into it.

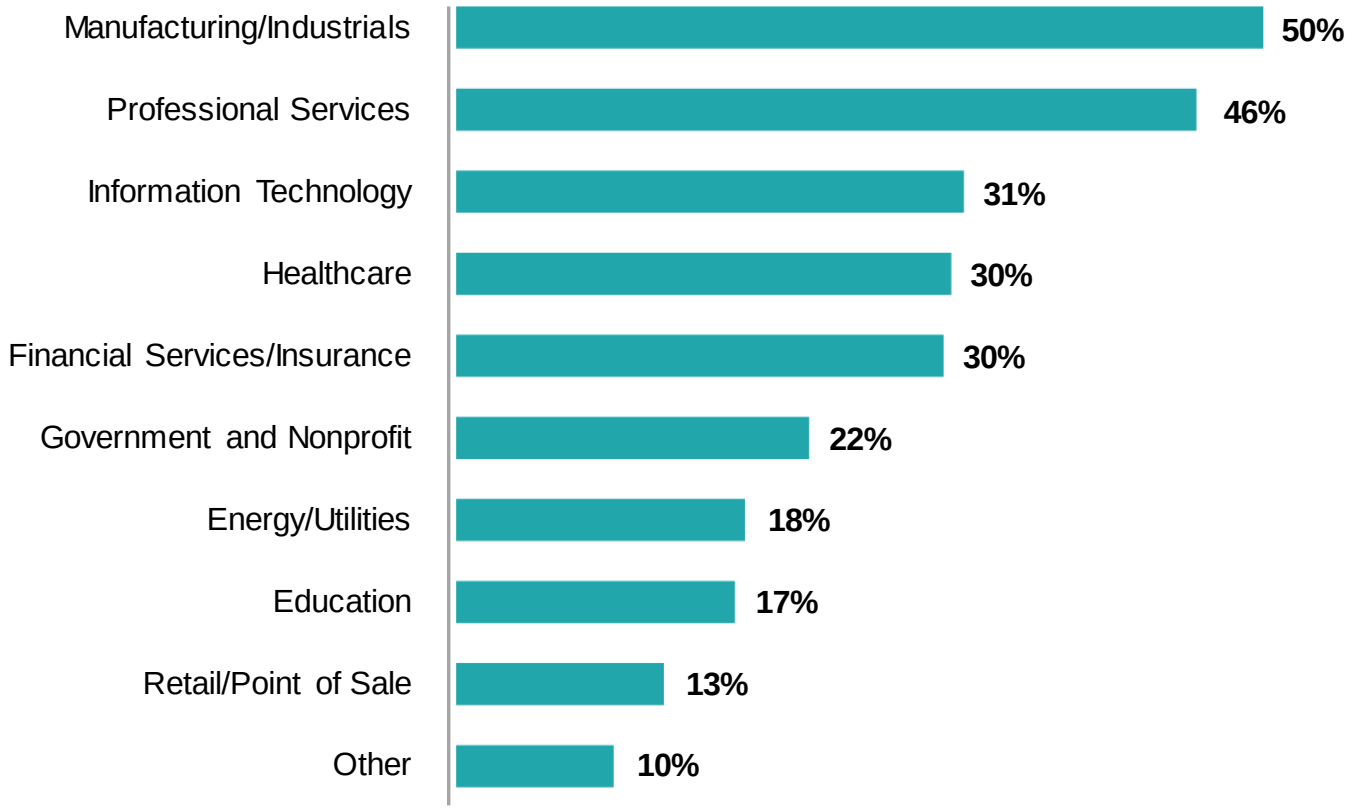
Of underwriters **analyze the systemic exposure** in their cyber portfolio.

Content Overview

Sales Motivations

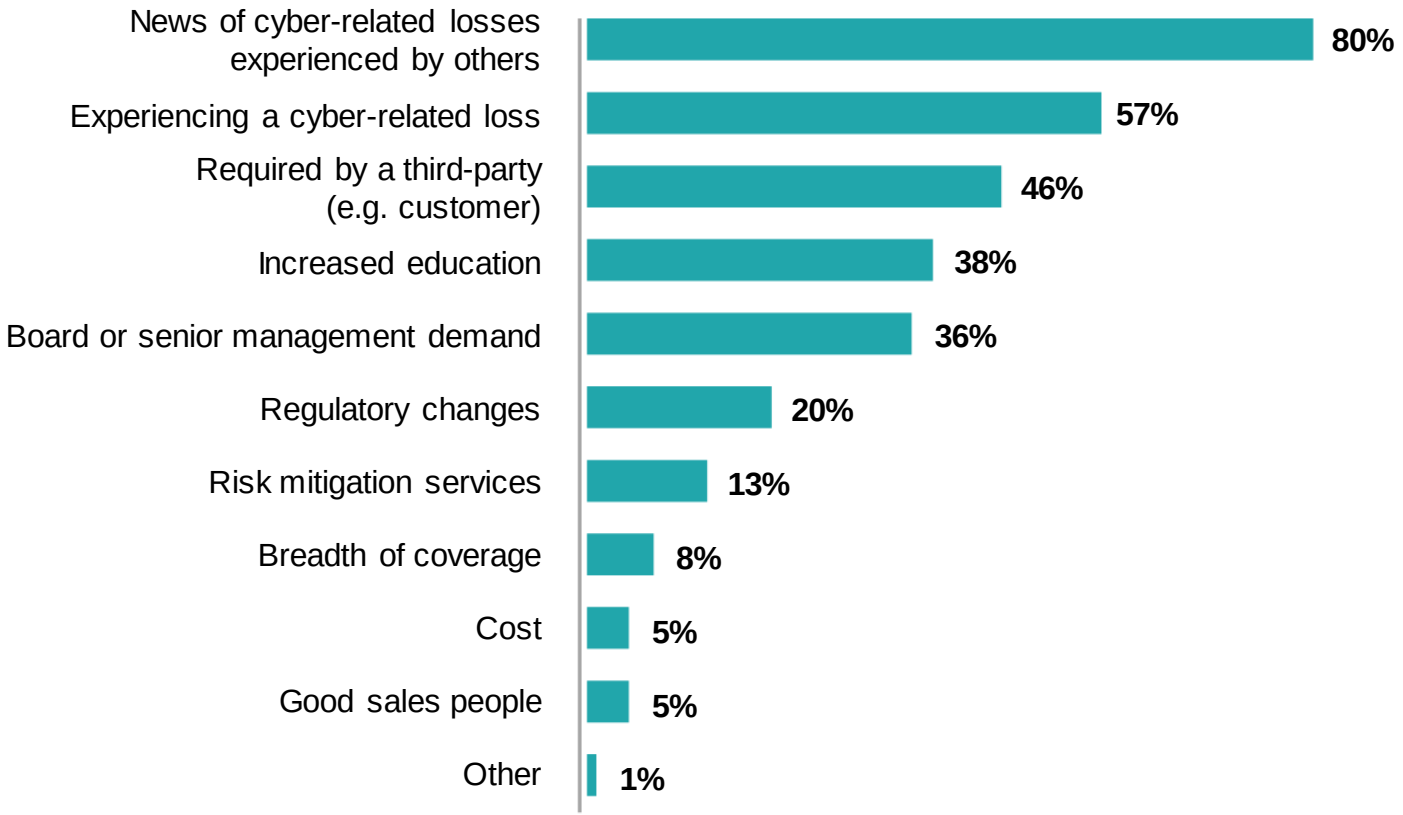
- The sectors bringing the most new buyers of cyber insurance is unchanged c.f. last year – “Manufacturing/industrials” and “Professional services” continue their lead.
- “News of cyber-related losses” increases its lead (+ 14 percentage points) as the top new/increased cyber sales driver.
- “Cost” continues its rise up the ranks as a major sales obstacle – now in 2nd place after 1st place “Not understanding exposures”. “Capacity constraints in the market” moves up from 7th to 5th place.
- Regulations (including the EU’s GDPR) are still not a key factor for cyber sales.

What industries brought the most new-to-market buyers of standalone cyber insurance? Please select top three.



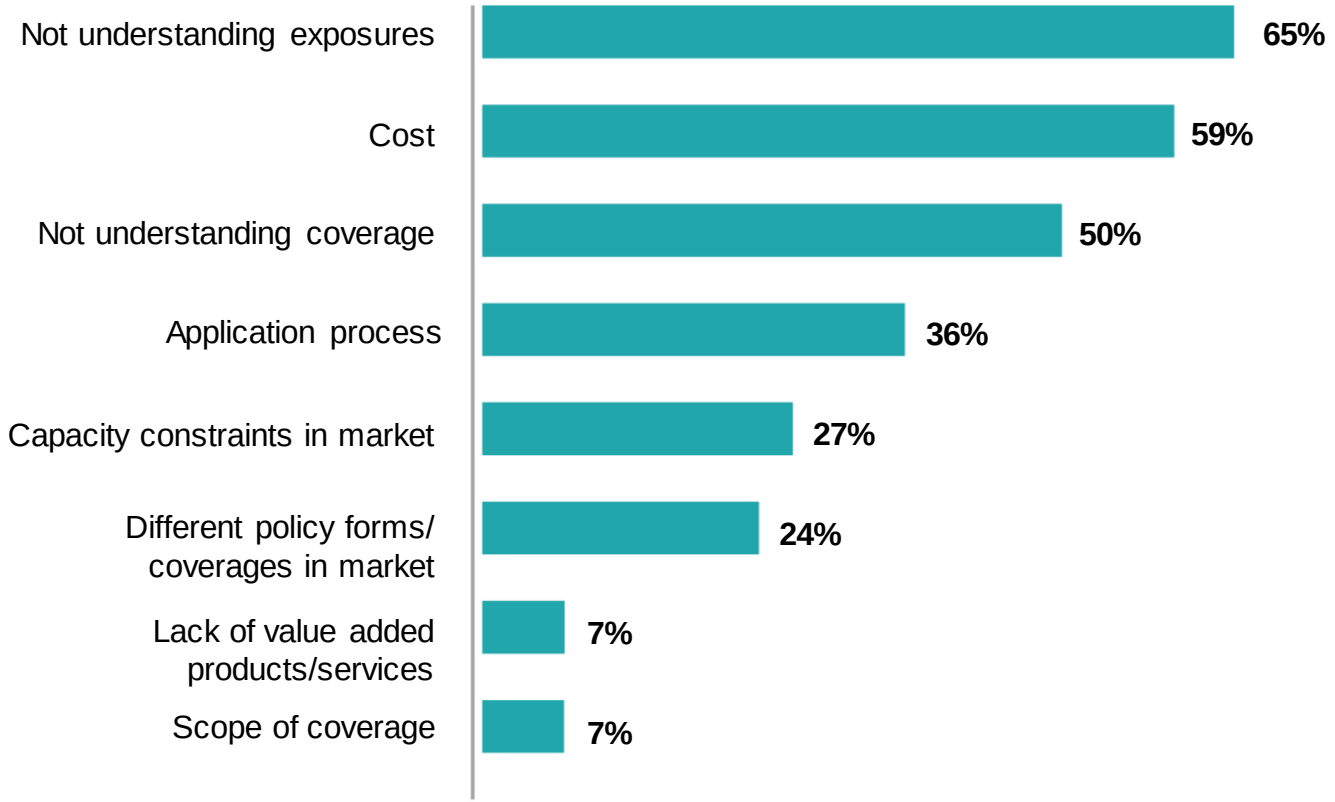
Results almost identical to last year, **some place shifting but no major moves** in terms of percentage. The incoming customer base by sector for cyber insurance therefore seems to be steady.

What do you see as the current top driver(s) of new/increased cyber insurance sales? Please select top three.



With evermore high-profile attacks, the top sales driver for the last 3 years, **"News of cyber-related losses" increased its lead** by another 14 percentage points. Other minor changes included "Required by third-party" which nudged upward, most likely due to prominent supply chain incidents, and "Regulatory change" which dropped a few points in line with the survey results on the impact of regulation (slides 9 and 36).

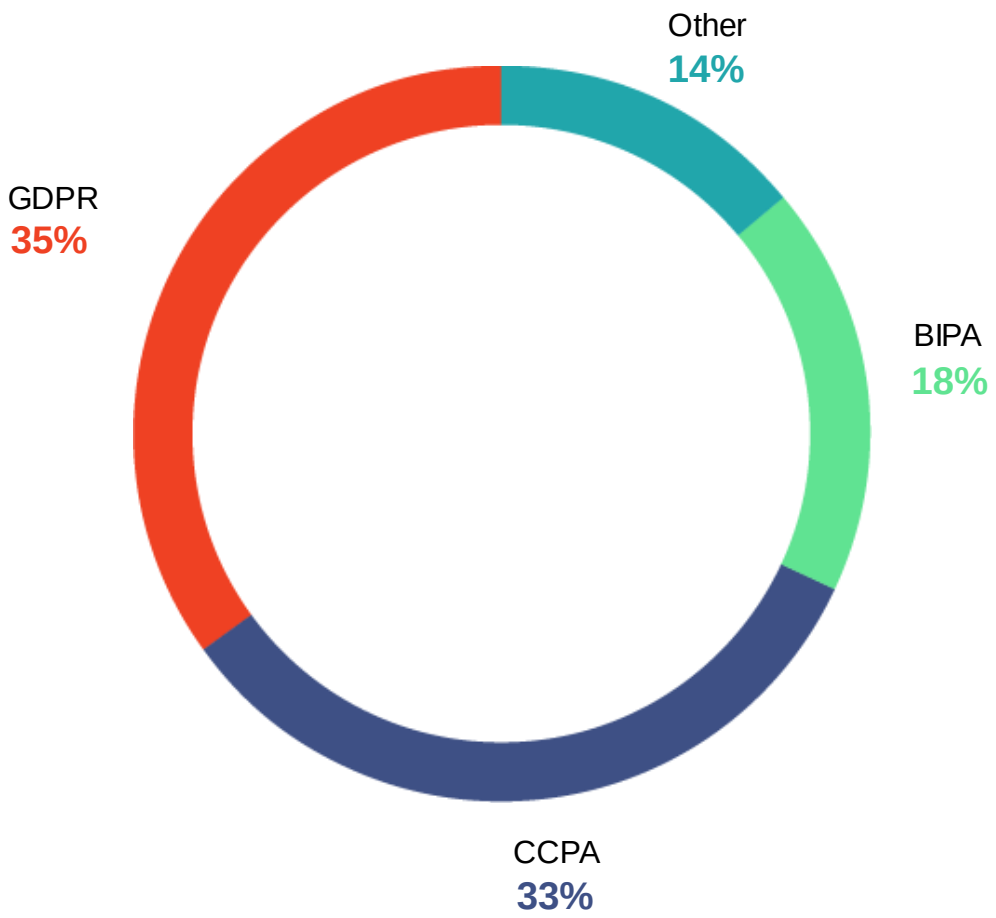
What are the biggest obstacles to selling cyber insurance? Please select top three.



Continuing a trend from last year, **"Cost"** rose another 9 percentage points to take second place. **"Capacity constraints in the market"** rose two places, gaining 16 percentage points. **Clearly a hardening market.** "Different policy forms/coverages in market" notably became less of an obstacle to sales (31% down to 24%), indicating improved coverage consistency, as slide 39 confirms.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

Which regulations do you think will have the largest impact on cyber sales? Please select one (BIPA, CCPA, GDPR, Other).



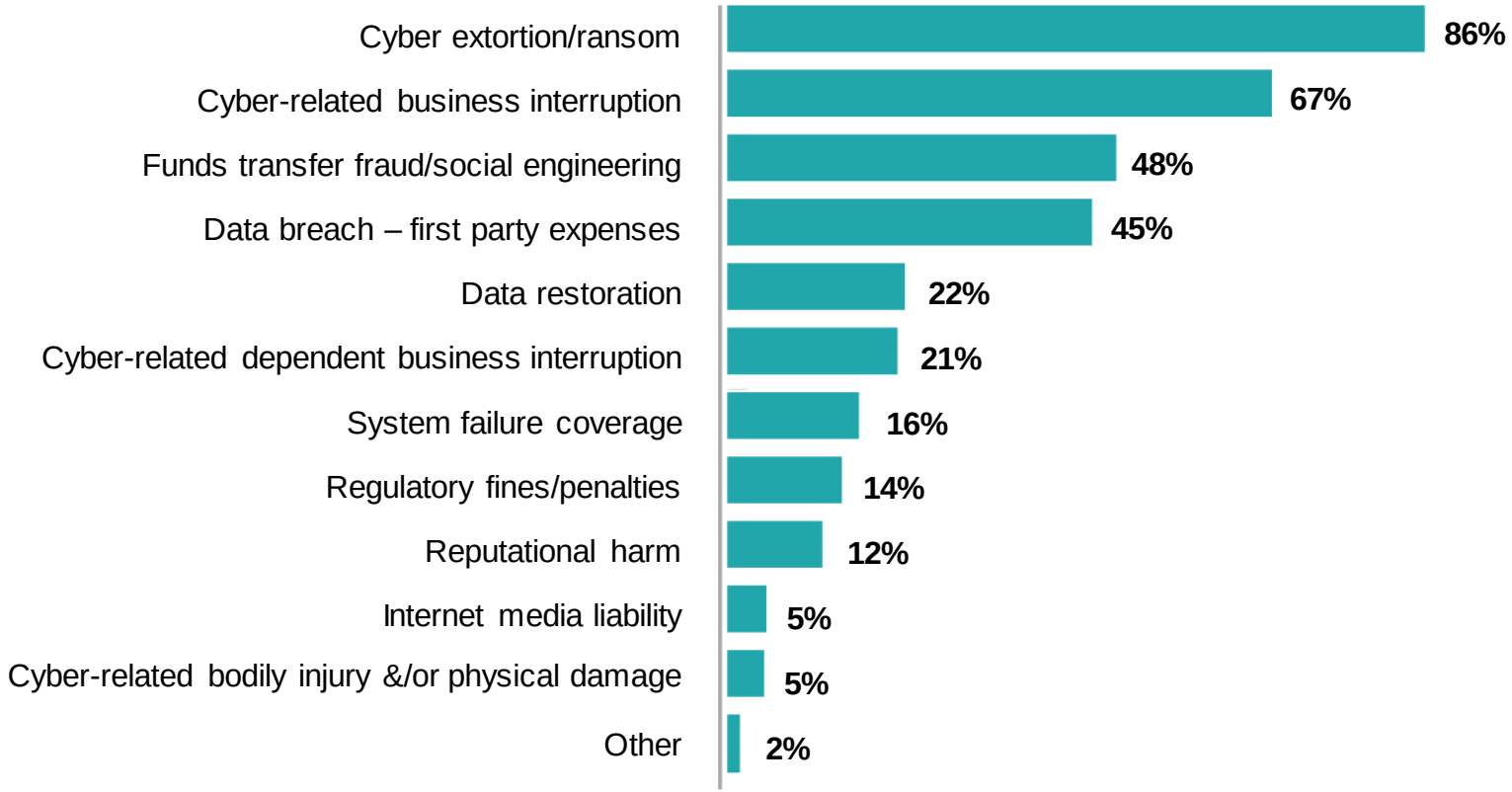
GDPR is still ahead, but only just. From the many comments and regulation's low position on the sales driver table (slide 7), regulations are in any case currently **not a key factor in cyber sales**. Fines and Penalties are often only covered under cyber insurance policies where insurable under local law, and to what extent such items are insurable remains untested.

"Not sure regulation is a driving force especially when you look at the take-up rate in the SMB medical community (given HIPAA's record fines the past 5+ years). Think immediacy of ransomware and potential for litigation are stronger drivers."

Coverage Requests

- “Cyber extortion/ransom” overtakes “Cyber-related business interruption” as the coverage that buyers are most interested in – 86% put this in their top-3. First-party exposures remain top of mind for buyers.
- Over half (53%) of respondents reported frequent demand for higher limits for all requested coverages.
- “Internet media liability” narrowly leads the table of coverages for which clients would consider reduced limits or exclusions in order to reduce premium – however, many respondents noted that, given the increasing loss frequency, reducing coverage is not the preference of buyers.
- Interest in cyber-related property damage and/or bodily injury coverage falls further – 47% “Rarely/Never” received requests for this c.f. 36% last year.
- Reinsurance is an increasingly important risk management tool – over half of those placing reinsurance reported an increase in requests for reinsurance.

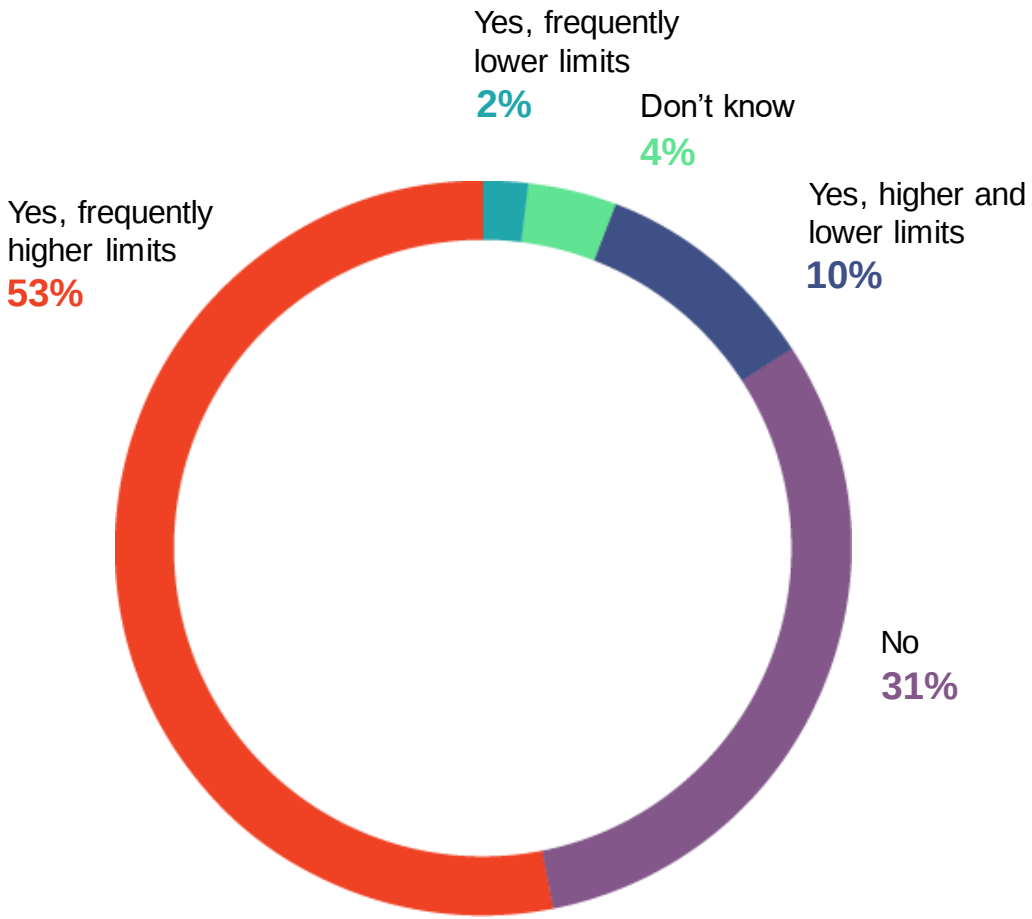
What cyber coverages are (new and renewal) buyers most interested in purchasing? Please select top three.



The big mover here was "Cyber extortion/ransom" which rose 26 percentage points to take the lead from the top-ranked coverage of the last 3 years, "Cyber-related business interruption". First-party exposures are top of mind for insureds.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

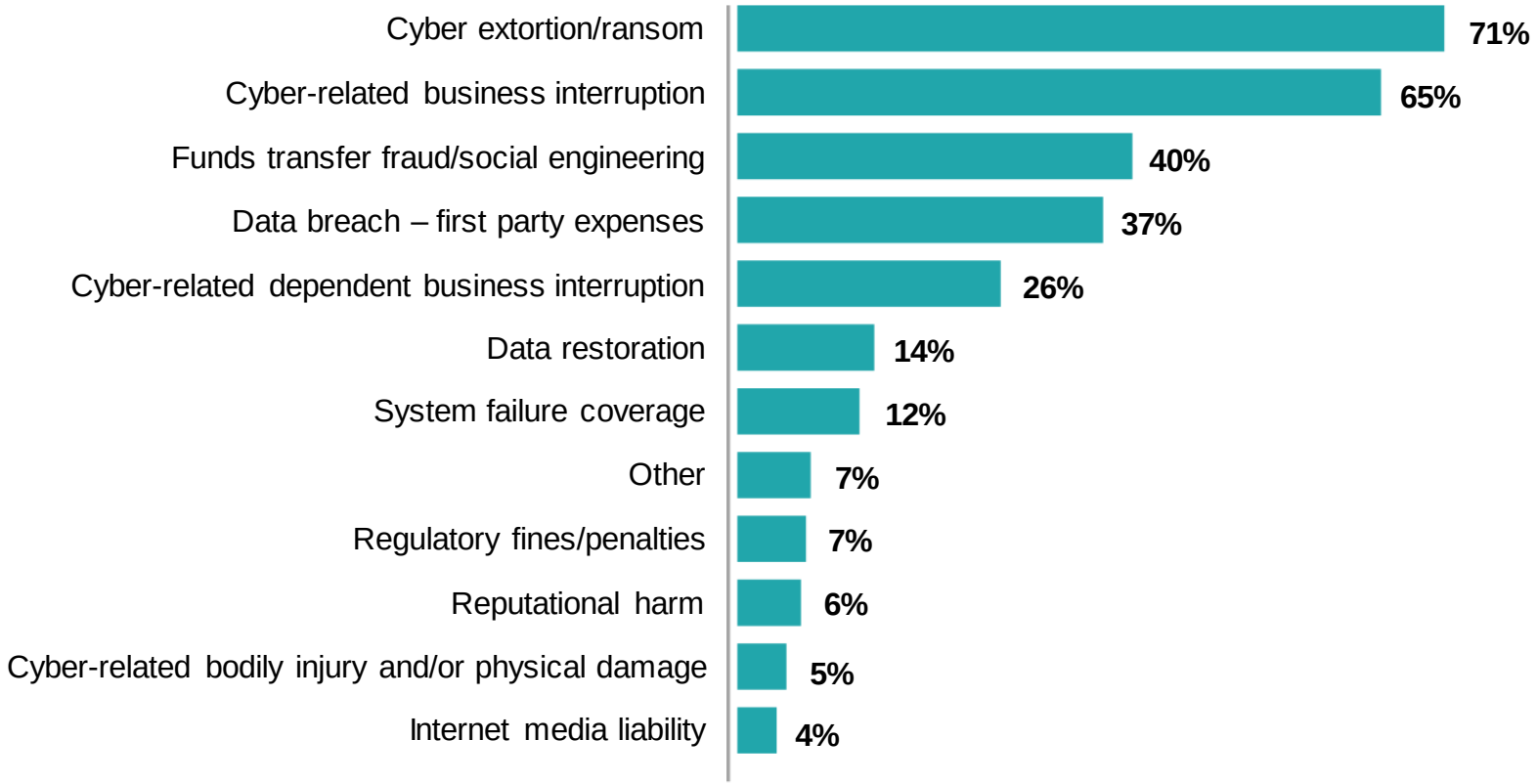
Are your renewal insureds frequently requesting different cyber insurance limits?



Similar to last year, **over half saw frequent demand for higher limits - increasing recognition of exposure clearly continues.** Comments indicated, however, that reduced capacity and cost are limiting what is actually purchased.

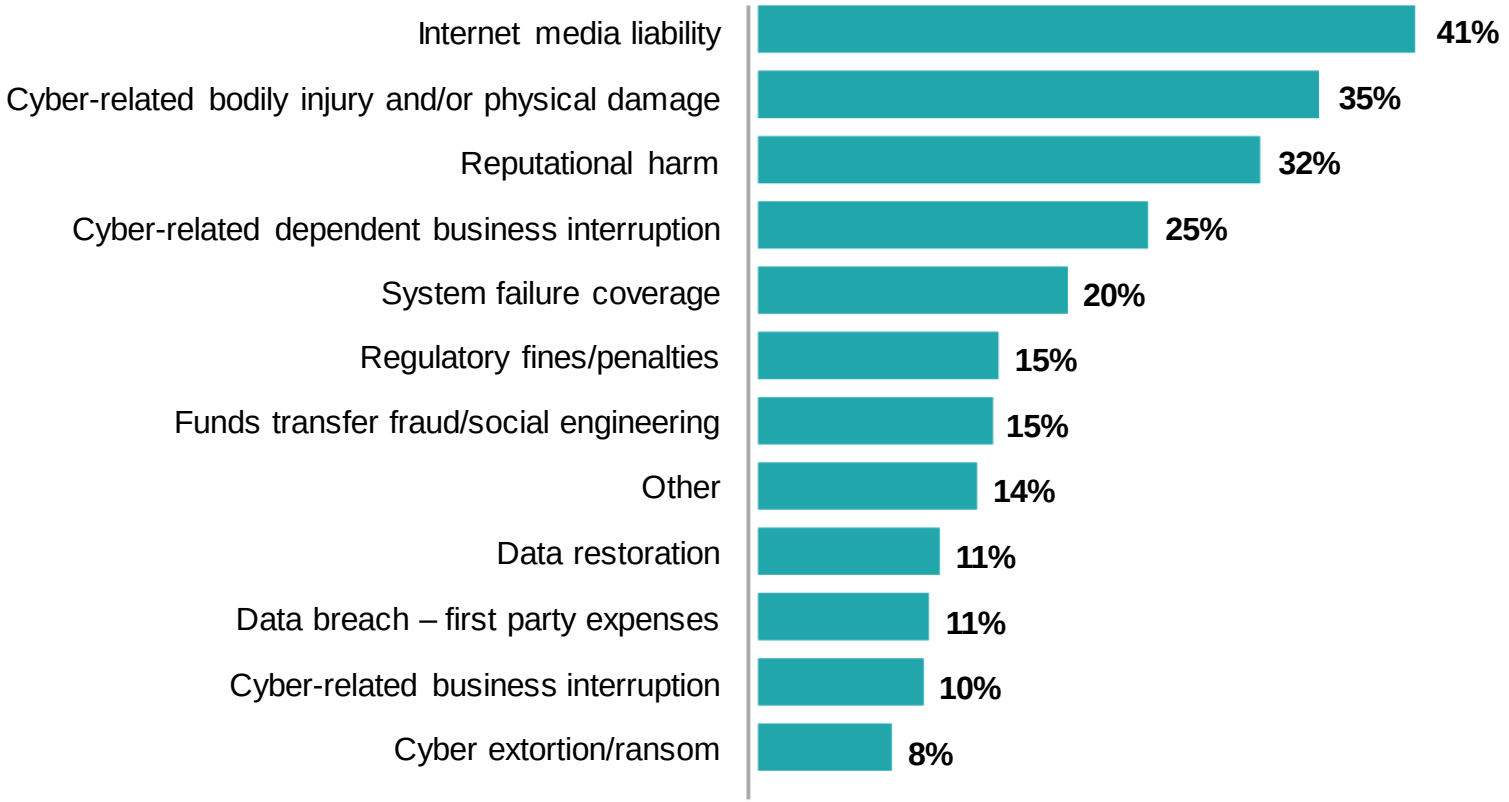
"The capacity is now reduced so clients buy what they can find; it is rather difficult to have clients looking for higher limits because it is a lot more costly and there is not enough capacity."

For which coverages are higher limits mostly requested? Please select top three.



The results mirror that of coverage requests, indicating that **higher limits are sought across the board, led by concerns for first-party exposures**. "Cyber extortion/ransom" holds the top spot; given the many well-publicized loss events, this exposure is well understood by clients and capacity is in high demand.

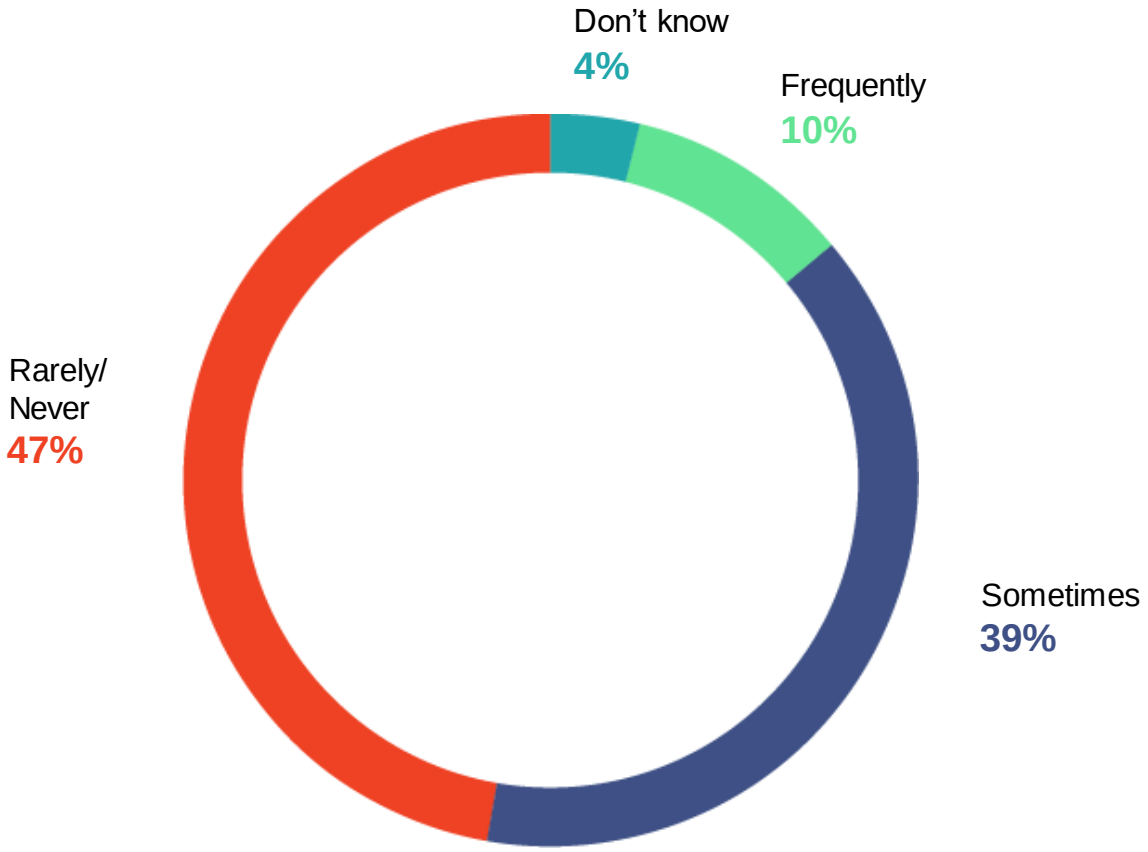
For which coverages are clients most likely to consider reduced limits or exclusions, in return for premium savings? Please select top three.



While these results are of interest, especially regarding Cyber-related BI/PD given ongoing discussions around the relevant policy, the overriding response here from comments was that, in particular given the increasing loss frequency, **clients do not want to reduce coverage, even for premium reduction.**

"Clients are not looking to reduce coverage, it's insurers who are dictating the reduction in coverage."

How often do you receive requests for cyber-related bodily injury and/or physical damage coverage?

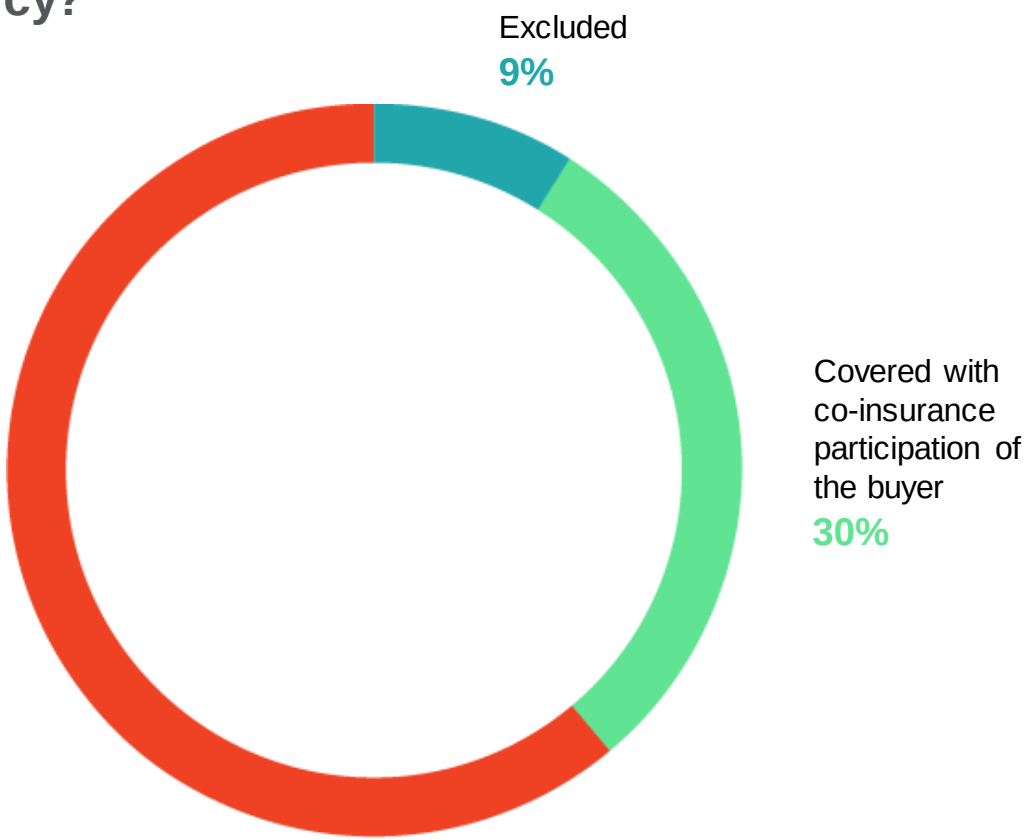


As predicted last year, **interest has fallen further** - last year "Rarely/Never" and "Sometimes" were neck and neck, this year "Rarely/Never" has an 8-point lead. The ongoing lack of headline events for this specific coverage is no doubt responsible, with lack of experience data and underwriter preferences for the property policy (see slide 18) likely also factors.

Coverage Specifics & Other Policies

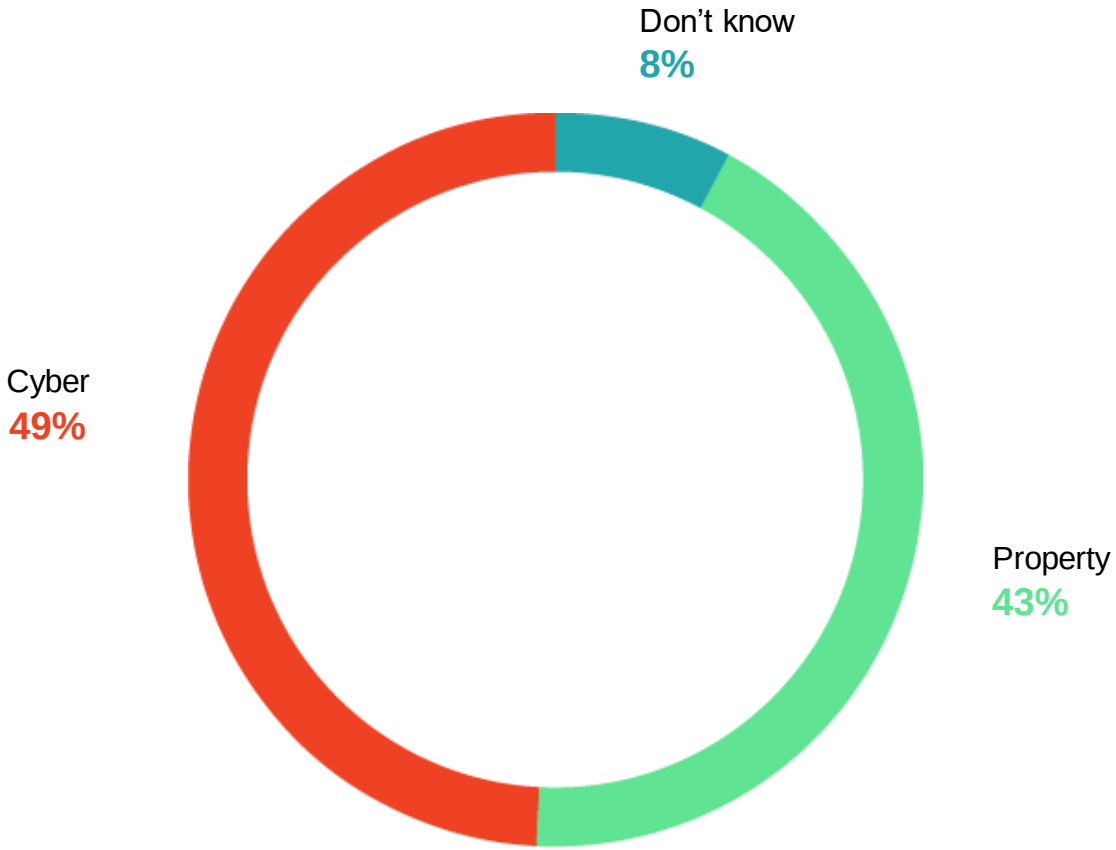
- 91% of respondents think that extortion demands, where insurable under law, should be covered. Exercising caution, almost half of underwriters said yes, but with coinsurance of the buyer.
- Opinions remain split on whether cyber-related property damage belongs in the cyber or property policy – underwriter respondents mostly (68%) prefer property, while broker respondents narrowly (55%) prefer cyber.
- The crime policy narrowly continues (55%) as the preferred policy for funds transfer fraud loss due to social engineering.
- Success with coverage clarity continues – 70% report that coverage overlap with other policies is the same or has decreased.

Do you believe that the payment of extortion demands, where insurable under local law, should be covered under or excluded from a dedicated cyber policy?



Covering extortion demands is the clear preference (only 9% overall wanting exclusion). **Underwriters were more cautious** here though, 23% wanting exclusion (compared to only 6% of brokers) and almost half opting for inclusion but with coinsurance participation of the buyer.

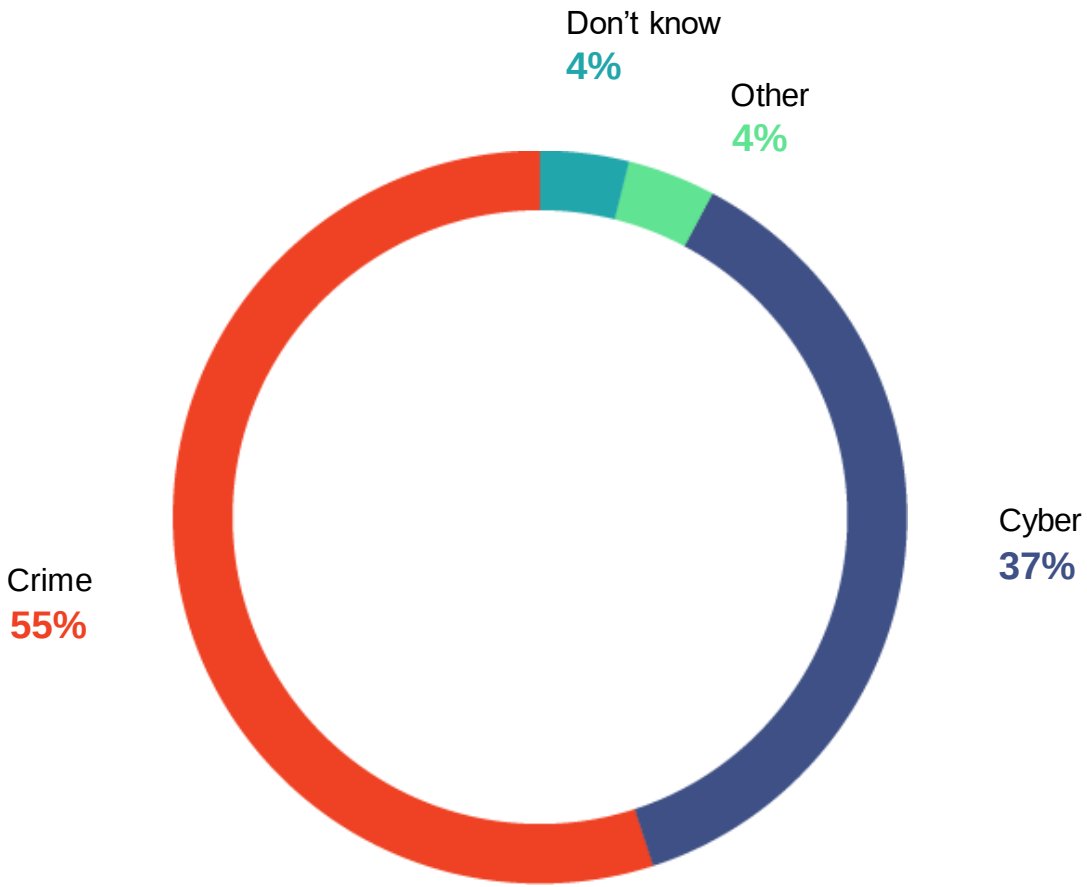
Do you believe cyber-related physical damage should be covered under a dedicated cyber cover or property policy?



Once again, **no clear winner**. With similar percentages to last year, brokers plump for "Cyber" (55%) while underwriters prefer "Property" (68%). Although "Cyber" narrowly takes the lead overall, several commenters were concerned by limits adequacy and capacity restrictions in the cyber market. Clarity and how losses are dealt with also stood out as decisive factors.

"Cyber policy will not give adequate limits for mega-industrial risks."

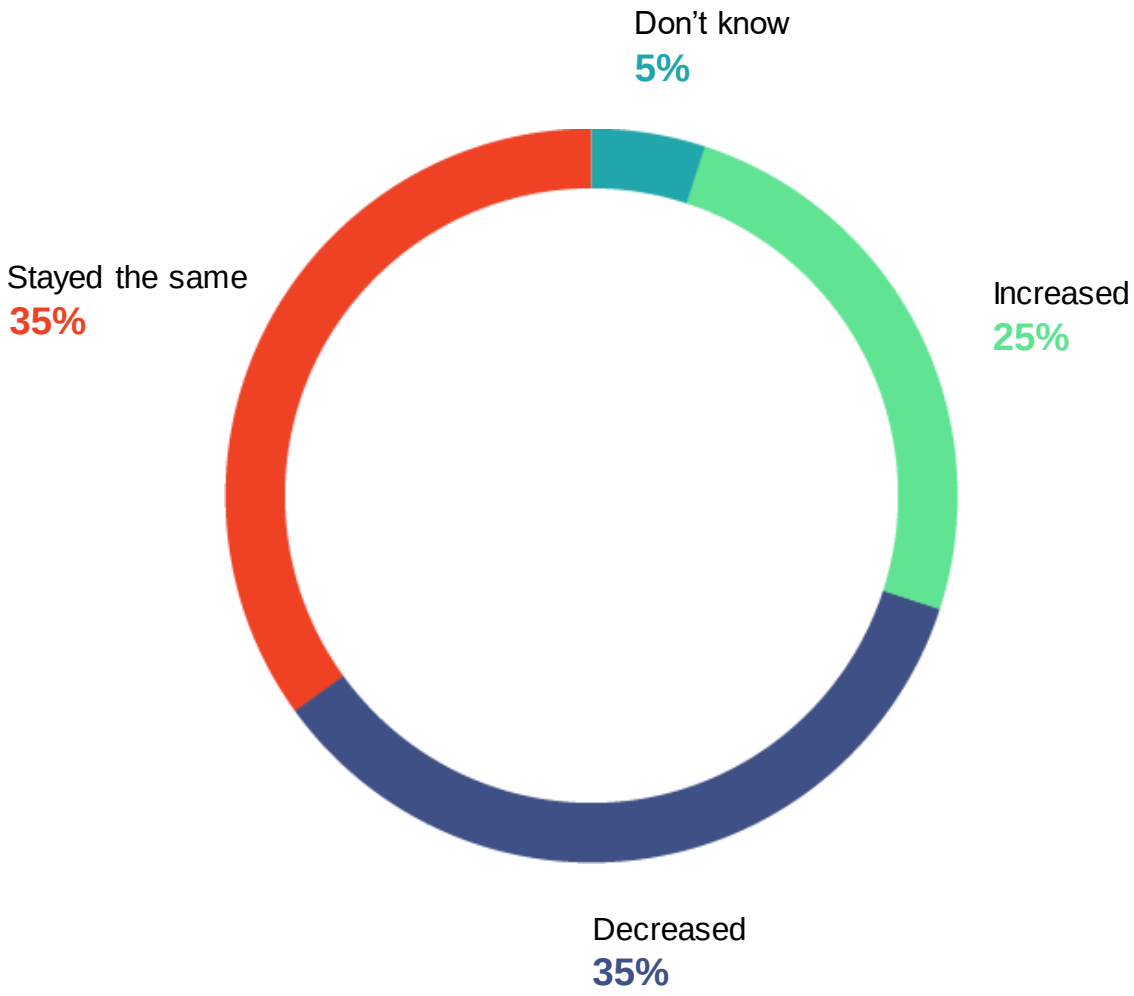
Where do you believe funds transfer fraud loss due to social engineering should be covered?



Underwriters and brokers continue to agree on **the crime policy**, perhaps as these policies have been seen to respond well to losses, though underwriters feel more strongly about this (70% opted for "Crime", versus 50% of brokers).

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

Coverage overlap between cyber and other policies has:



The results are **a good indication of continued success with coverage clarity**. That 25% note increased overlap may seem high, but in our 2018 survey this was 51%, so the overall trend is one of reducing overlap.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

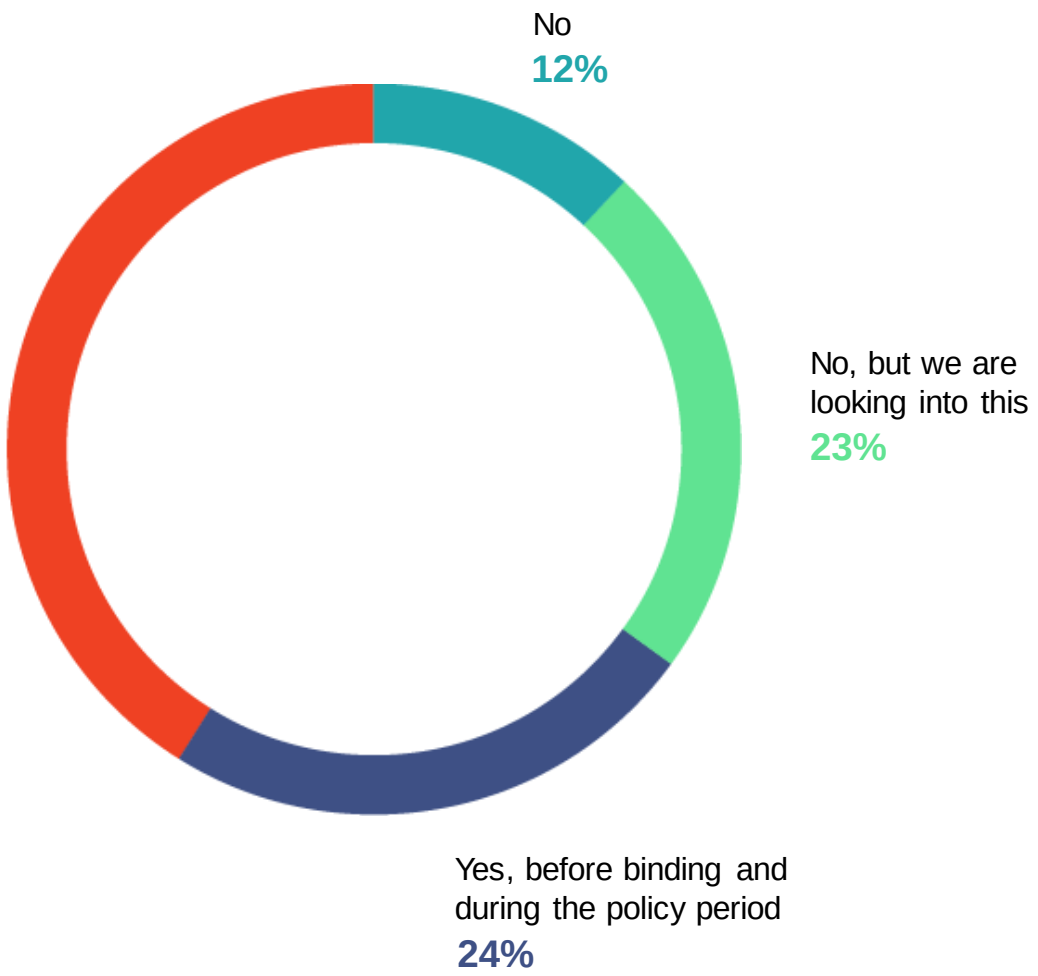
Survey Findings

Underwriting & Risk Aggregation

- 76% of underwriters actively manage cyber risk aggregation.
- 80% of underwriters utilize cyber risk models.
- Risk scanning is firmly established in underwriting – 65% do this already and a further 23% are looking into it. Also used proactively by clients to identify vulnerabilities and improve risks.
- Aggregation management “Always” or “Sometimes” impacts the underwriting decisions of 78% of underwriters.
- 95% of underwriters analyze the systemic exposure in their cyber portfolio.
- Just under half of underwriters are using delegated authority agreements to some extent – and of those that do, most (66%) are auditing them annually.
- Third-party vendors continue to be strategically used by 81% of underwriters for risk analysis and selection, and for a broad spectrum of uses, led by “Risk scanning” (31%) and “To identify top risk factors” (18%).
- 58% of underwriters are concerned by non-affirmative cyber in specialty property.
- This year saw a slight increase in carriers providing cyber-related bodily injury and/or property damage in their cyber policy, despite underwriter preferences for the property policy.
- 54% of underwriters have not made notable changes to their ransomware coverage – of those that have, this was mostly (60%) to reduce the sublimit.
- 73% of underwriters offer funds transfer fraud loss due to social engineering coverage in their cyber policy, despite 70% preferring the crime policy.
- Despite several publicized fines, as coverage response remains unclear, the GDPR is not causing any major shifts in the market.

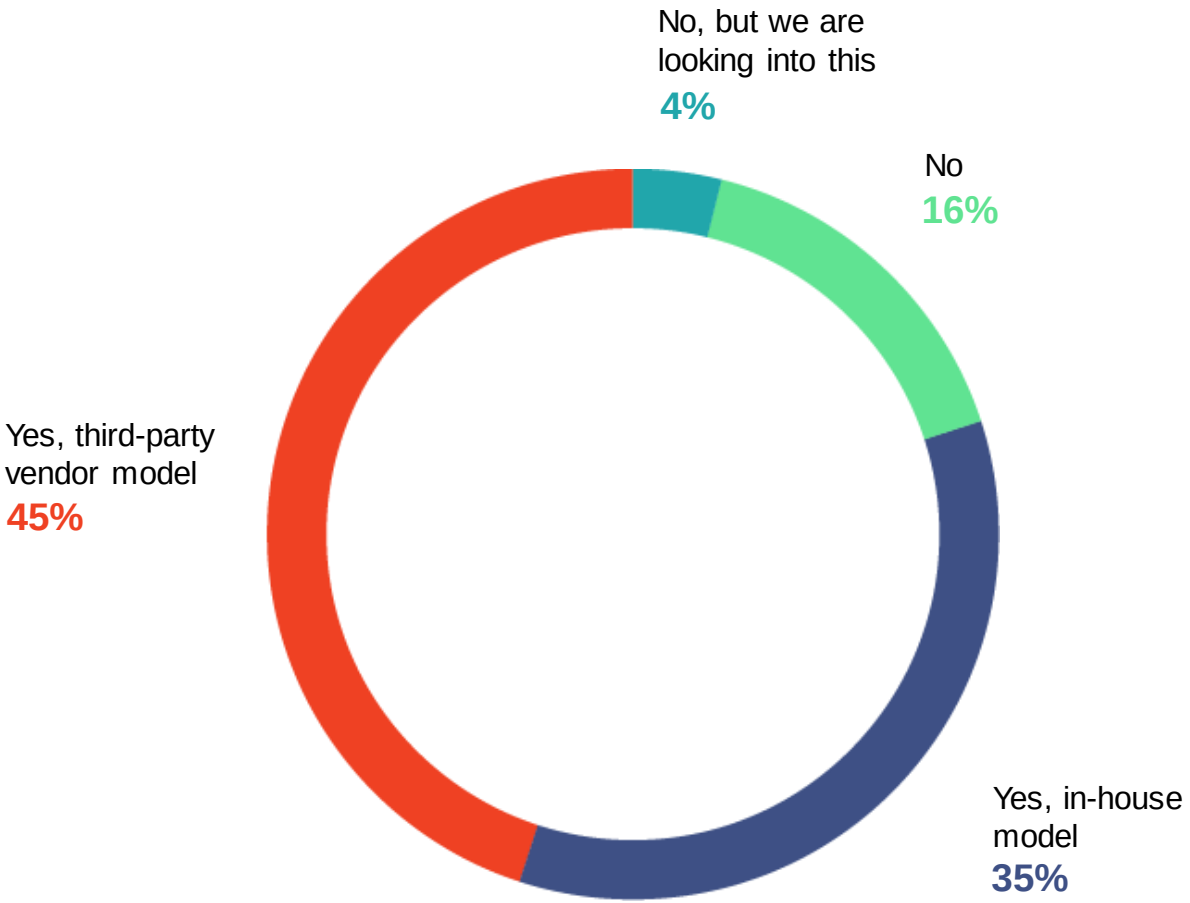
Note: All questions in this section, apart from the final question about the GDPR, were asked only to underwriters.

Do you scan the risks you underwrite to help detect vulnerabilities (in-house or via a third-party vendor)?



Risk scanning is firmly established and set to expand further as a risk assessment and risk mitigation tool, especially for larger risks. Comments also noted that clients are also doing this to proactively identify their vulnerabilities and improve the risks they present to market.

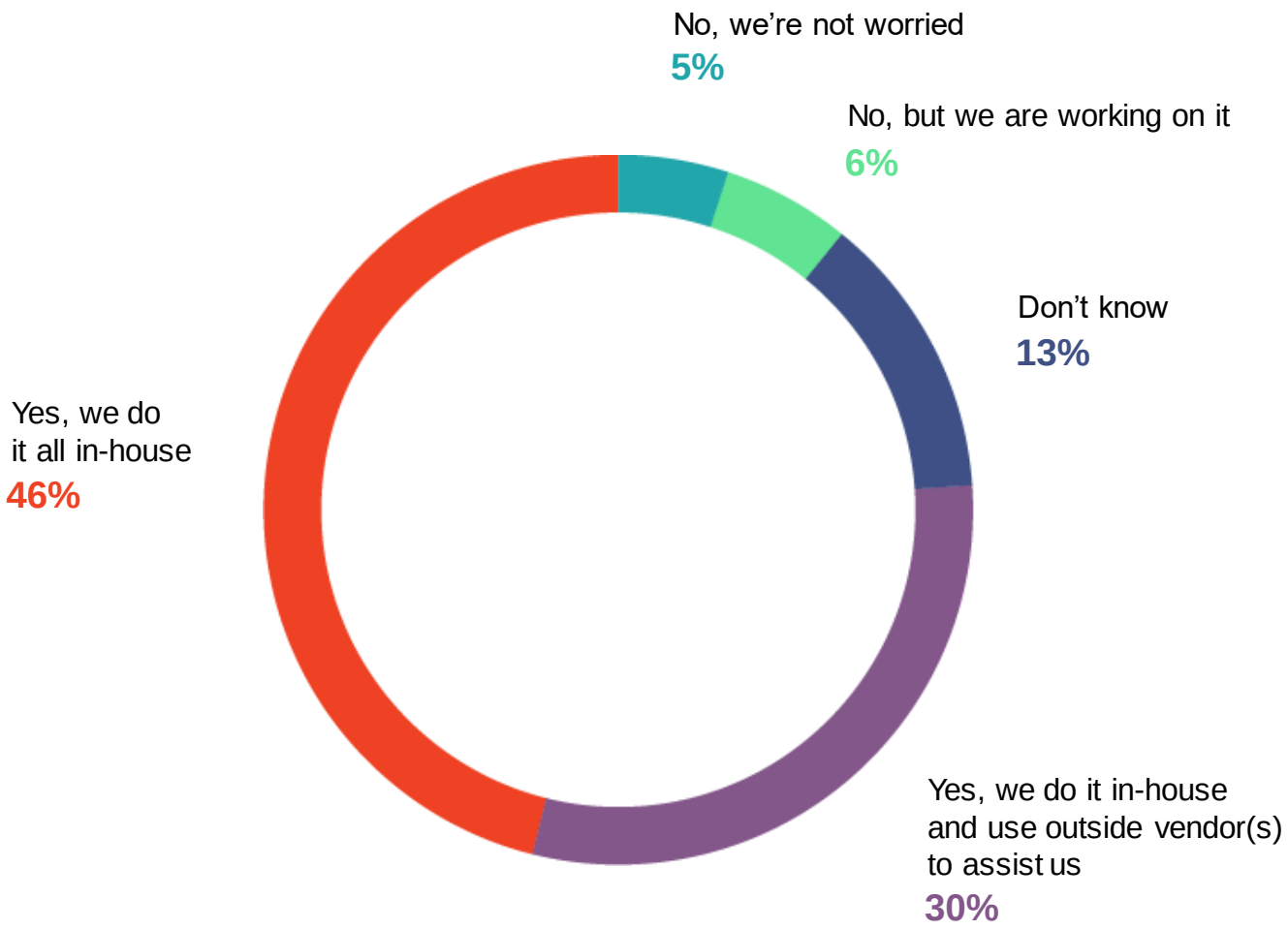
As part of your underwriting and portfolio management, do you also utilize cyber risk models?



Cyber risk models are also **in full use** across the industry.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

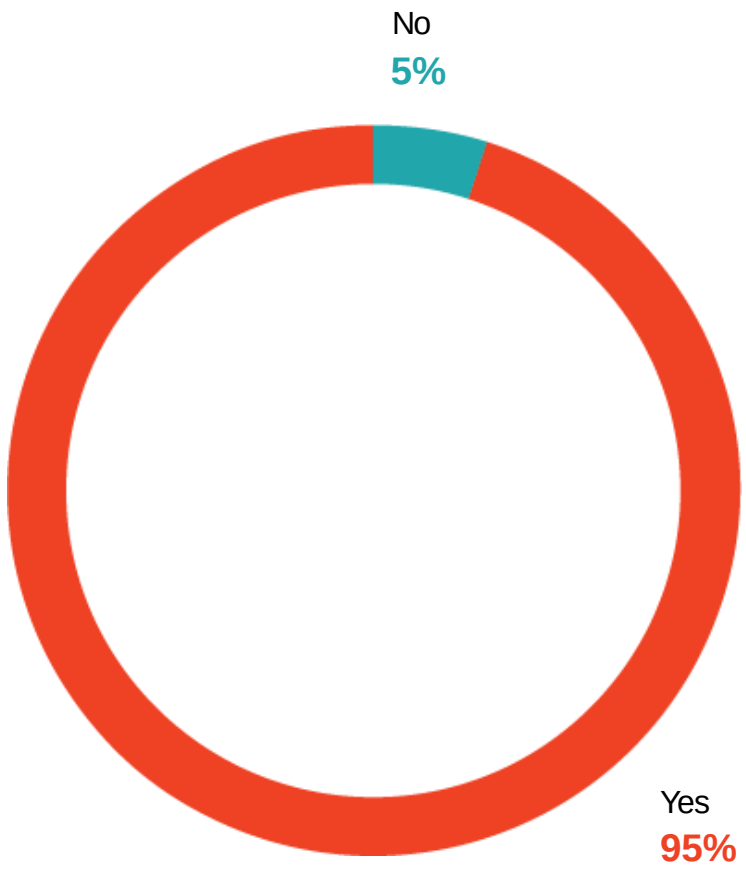
Is aggregation actively managed by your company?



Responses were similar to last year, with the **majority actively managing cyber risk aggregation**. Risk scanning (slide 22), use of cyber risk models (slide 23) and controlling ransomware exposure (slide 34) all corroborate this result.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

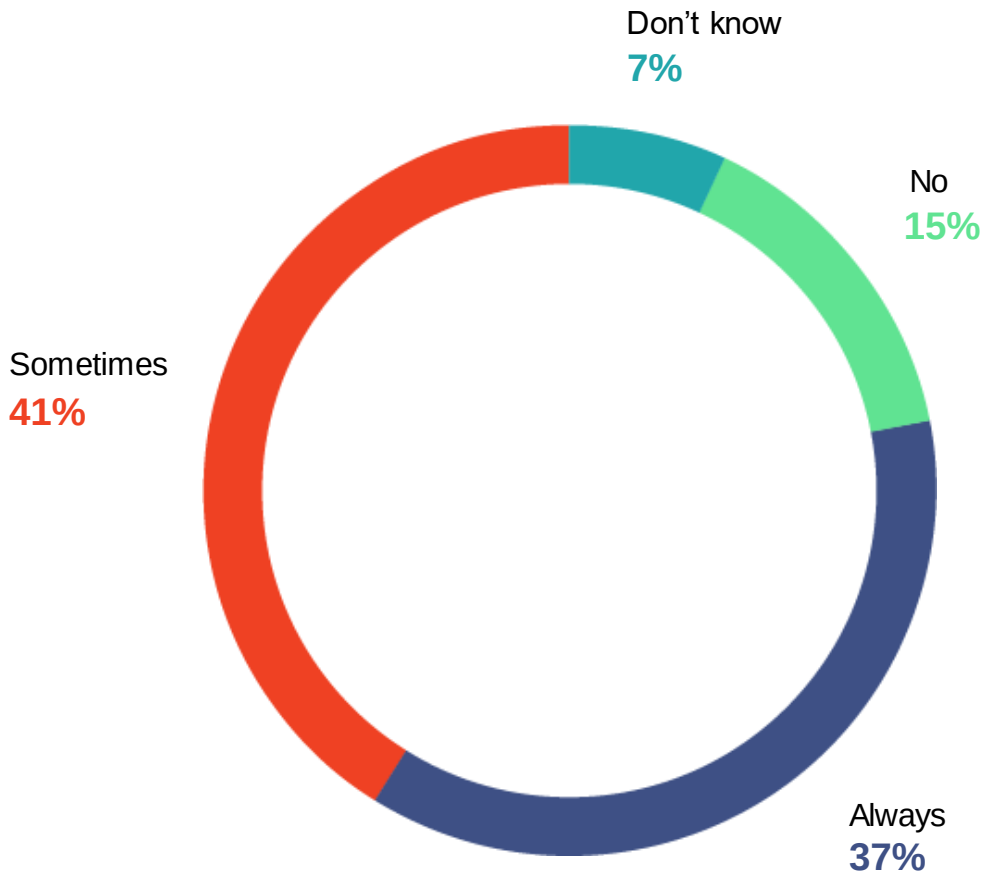
Do you analyze the systemic exposure within your portfolio?



As last year, **over 90%** recognize the need to analyze the systemic exposure in their cyber portfolio.

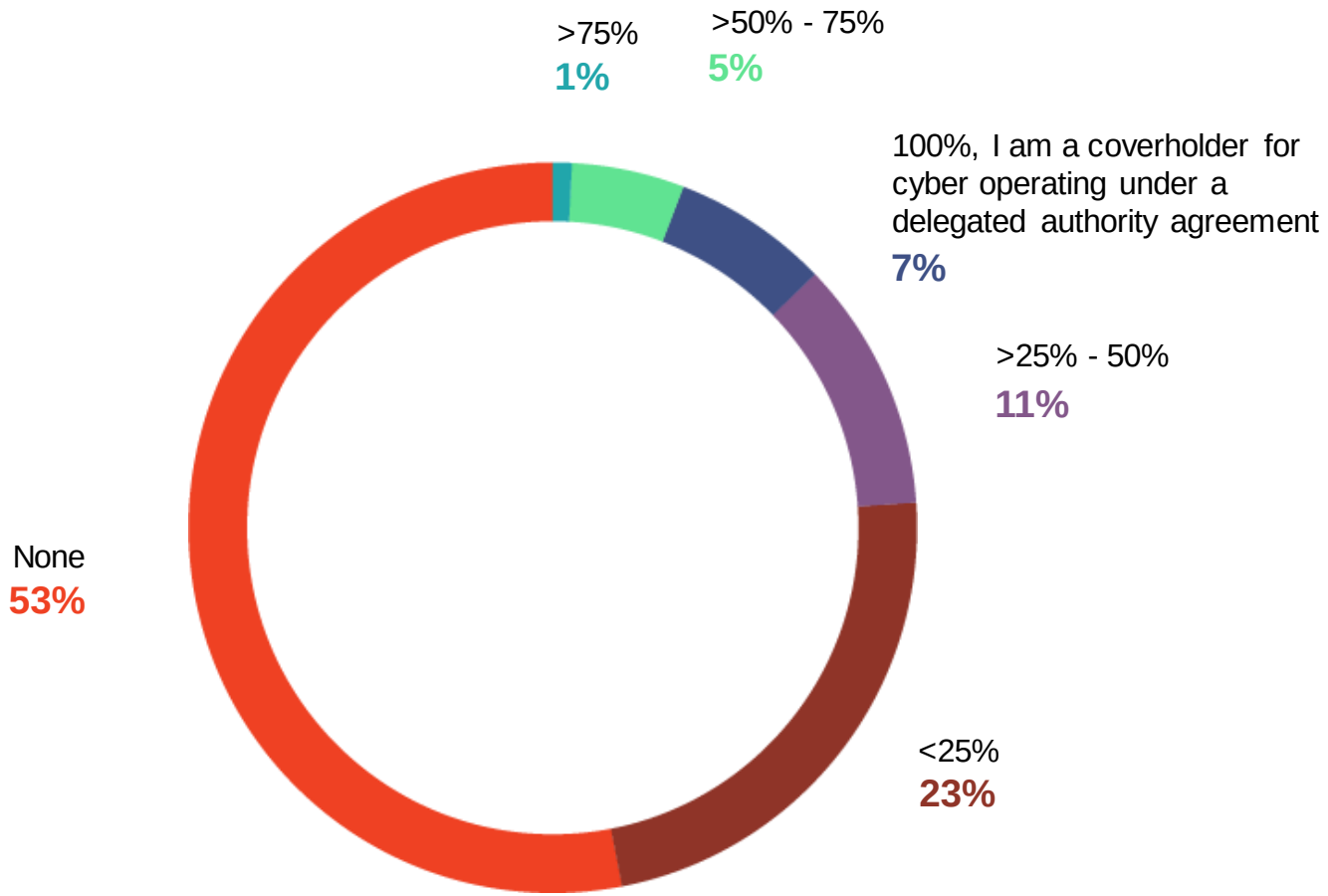
PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

Does aggregation management impact your underwriting or pricing decisions?



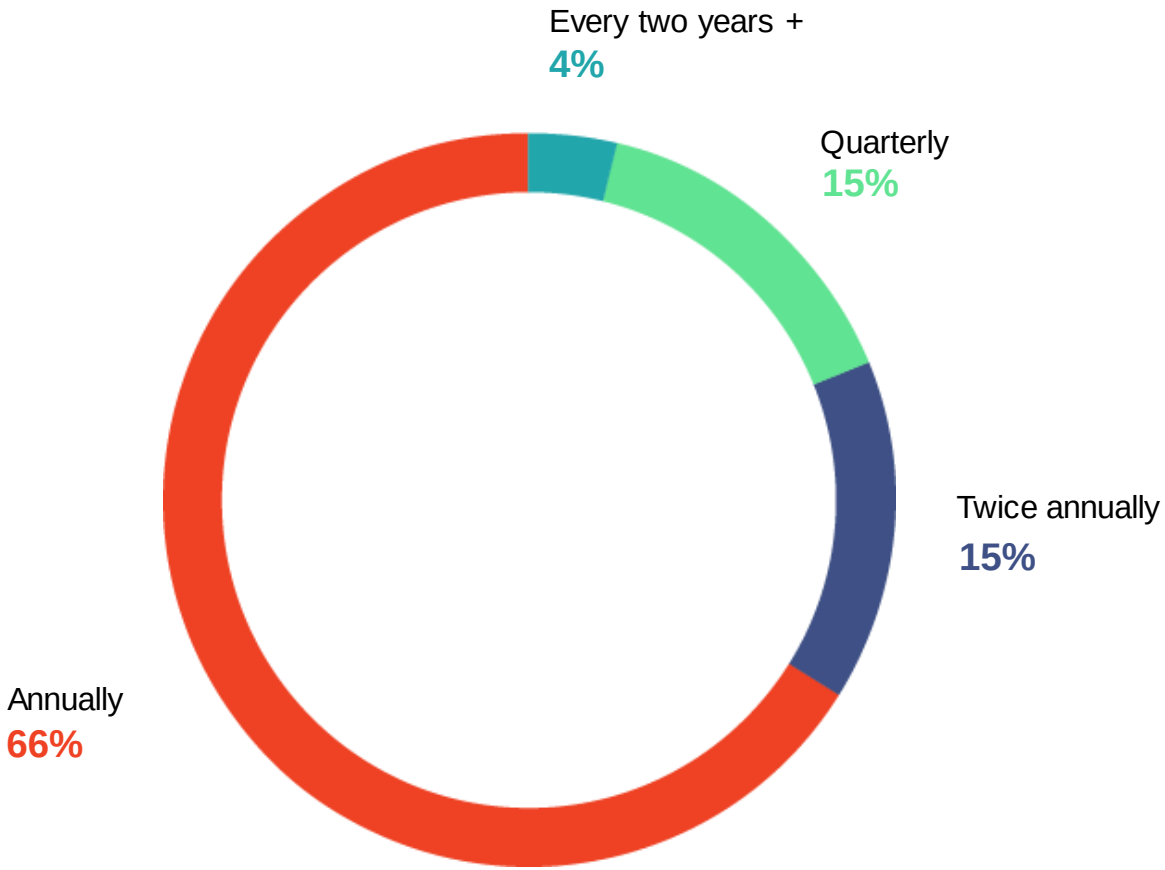
Compared to last year the **"Always" response is unchanged**. The "Sometimes" response, however, has fallen by 10 percentage points, a percentage gained by the "No" category. This slight shift reverses a 3-year trend, though it seems likely that this small change reflects an increased certainty of process, rather than a shift in behavior.

Approximately what percentage of your cyber portfolio GWP is produced via delegated authority agreements?



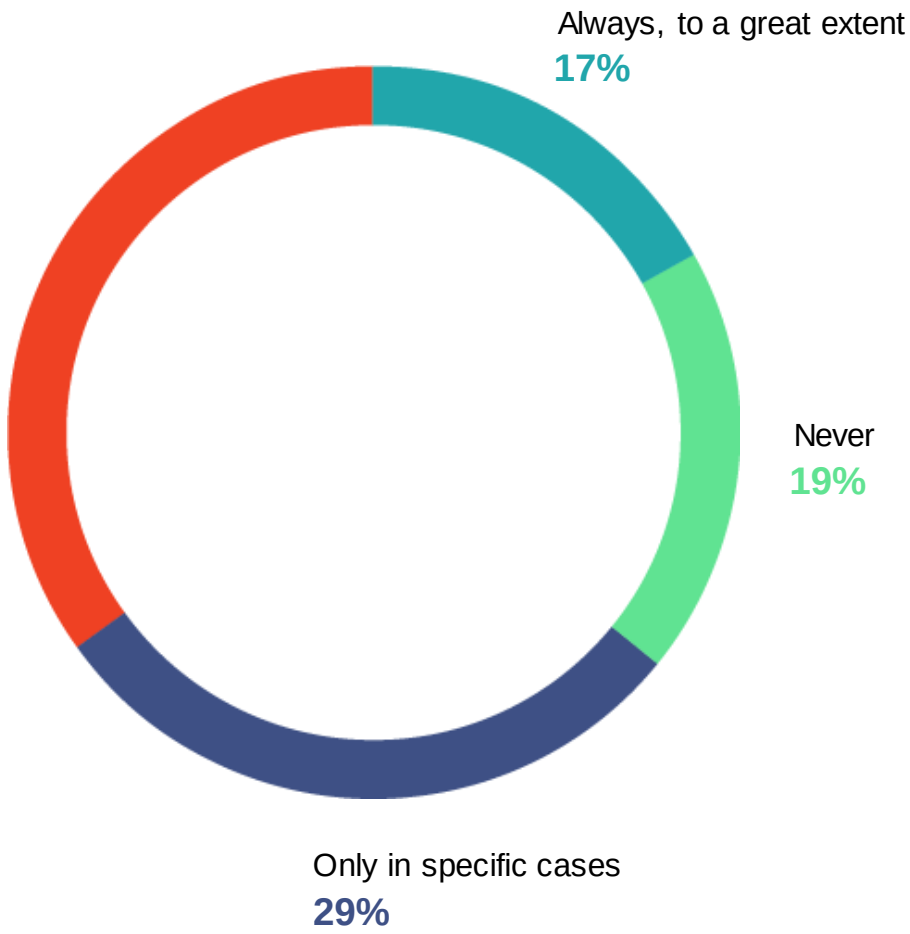
Just under half of respondents are using delegated authority agreements to some extent. This will be an interesting trend to watch.

How often do you perform underwriting and claims audits on your delegated authority partners?



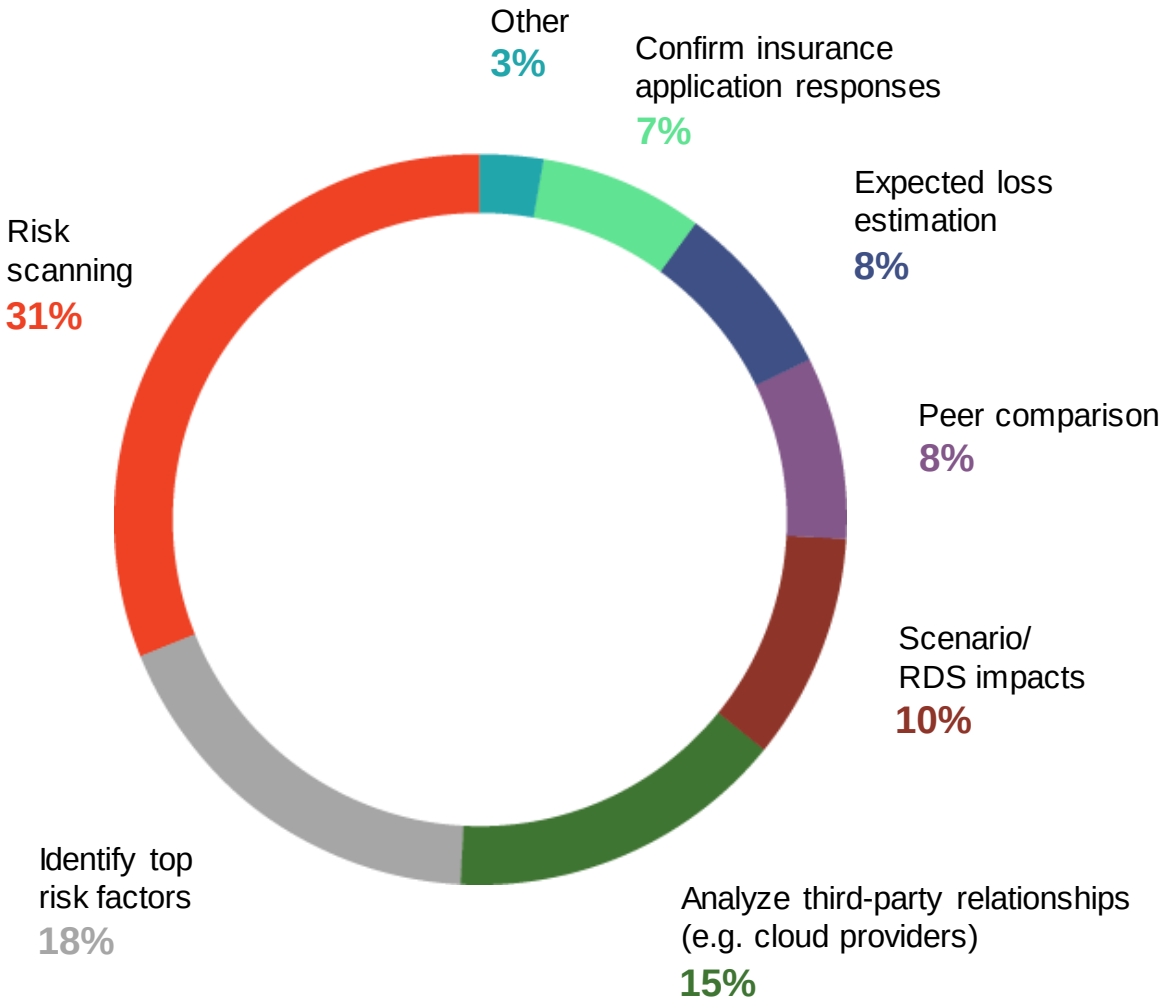
Of those answering this question, **annual audits** are considered by most to be adequate.

To what extent do you use third-party vendors for risk analysis and selection during the underwriting process?



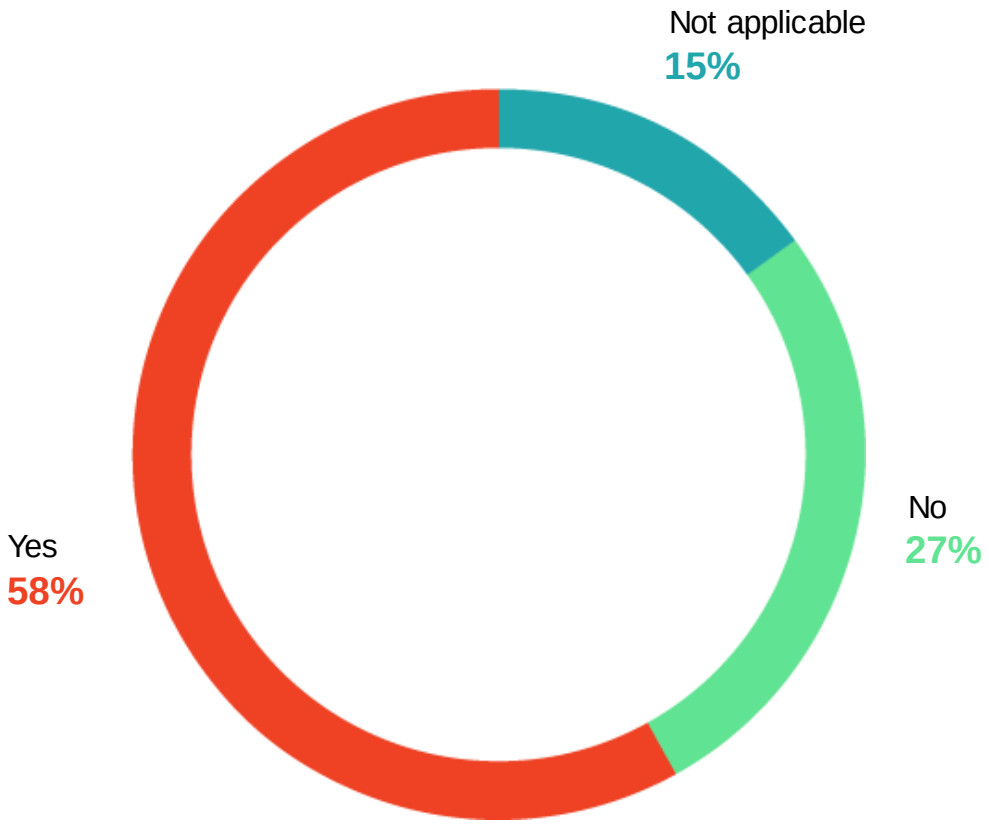
Similar results to last year, though "Always, to a great extent" gained 6 percentage points, while "Never" fell 6. Third-party vendors clearly offer value and are **being strategically used by underwriters**.

What are your primary uses of vendor products during the underwriting process? Please select up to three.



The top 2 results, **risk scanning and to identify top risk factors, indicate where underwriters see the most need for support**, but the broad spectrum of usage is also apparent. How this trends will be interesting to watch, especially given the slight increase in the use of third parties for risk assessment and selection (slide 29).

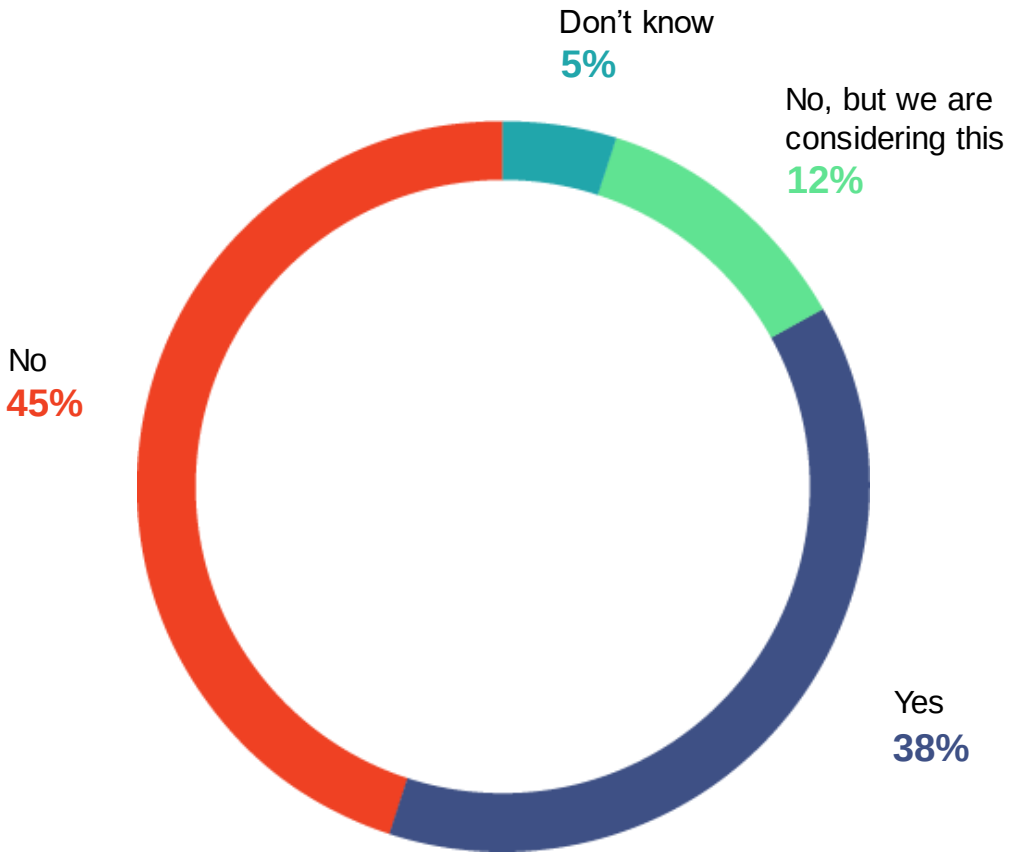
Are you concerned by non-affirmative cyber coverage present in specialty property risks?



Concern remains the dominant response of underwriters.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

Does your company's cyber insurance provide coverage for cyber-related bodily injury and/or physical damage losses?

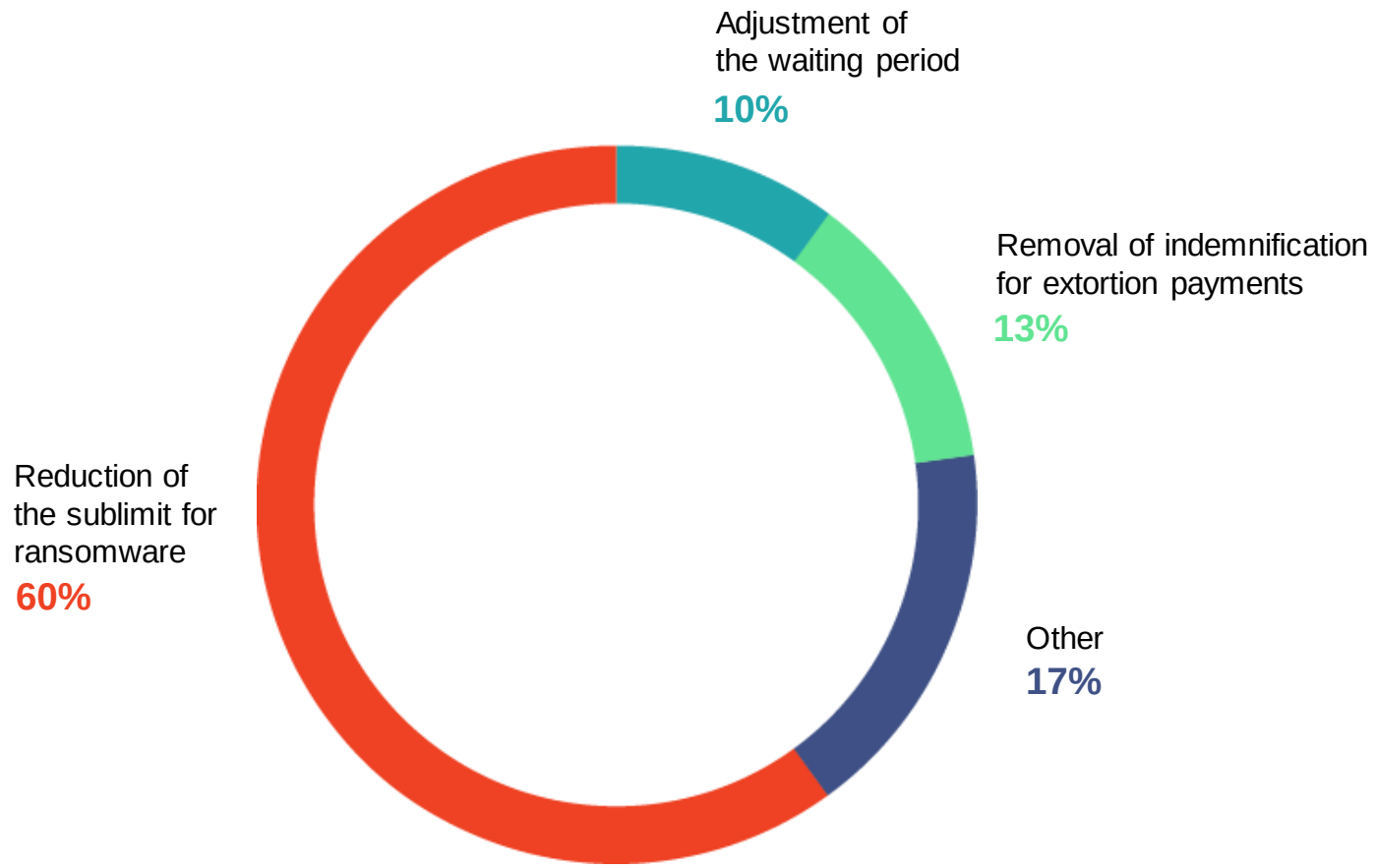


"No" remains constant c.f. last year, while **"Yes" has gained**, seemingly at the expense of those who were considering it, signaling a slight shift towards offering this coverage within the cyber policy. This is interesting given that most underwriters prefer the property policy (slide 18), but likely indicates recognition of the need for flexibility.

Have you made any notable changes to your ransomware coverages?

Split response is interesting – see following slide for why and what changes are being made. That approximately half are not making changes could reflect that the cover is deemed appropriate and risk management is strong.

What do the changes to your ransomware coverage primarily aim to achieve?

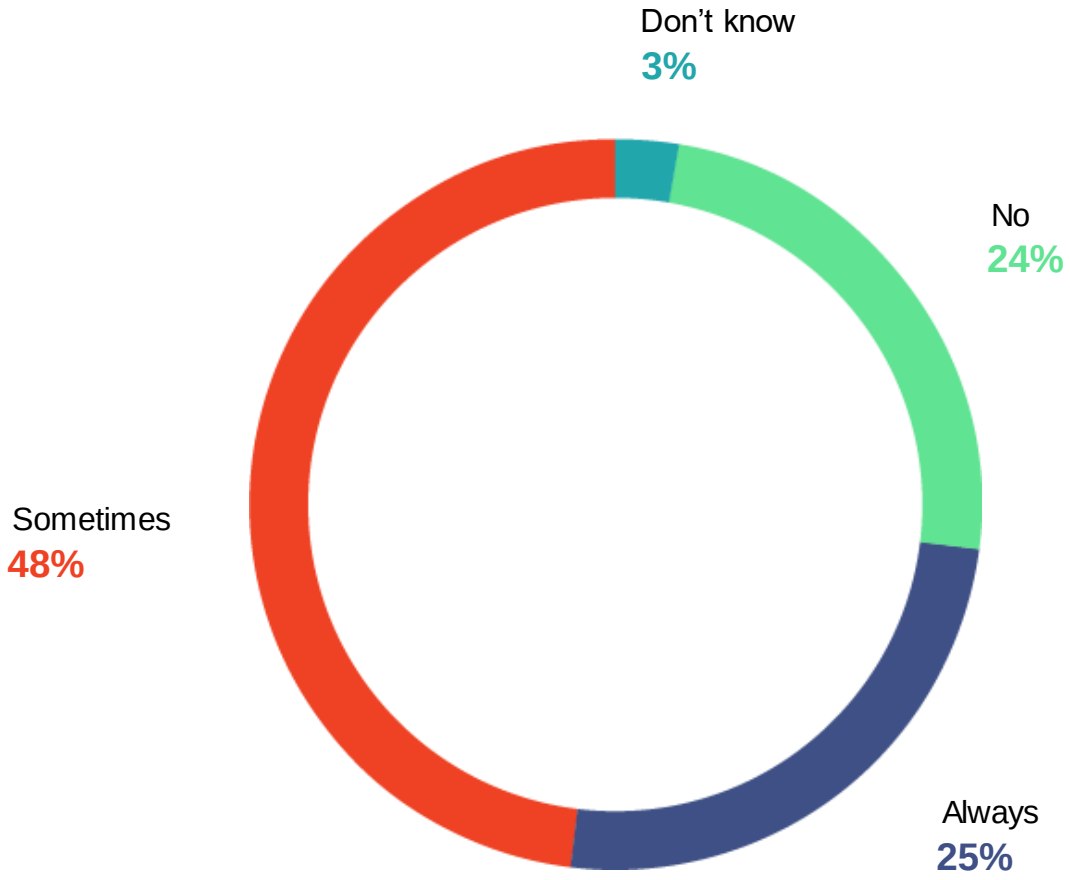


Reducing the sublimit leads as a risk management tool. Comments added coinsurance and increased retentions to the toolbox.

"Depending on the type of risk and controls in place we would use a variety of tools to manage the exposure to include sub-limits, increased retention, coinsurance, excluding the coverage or in some cases offering full coverage."

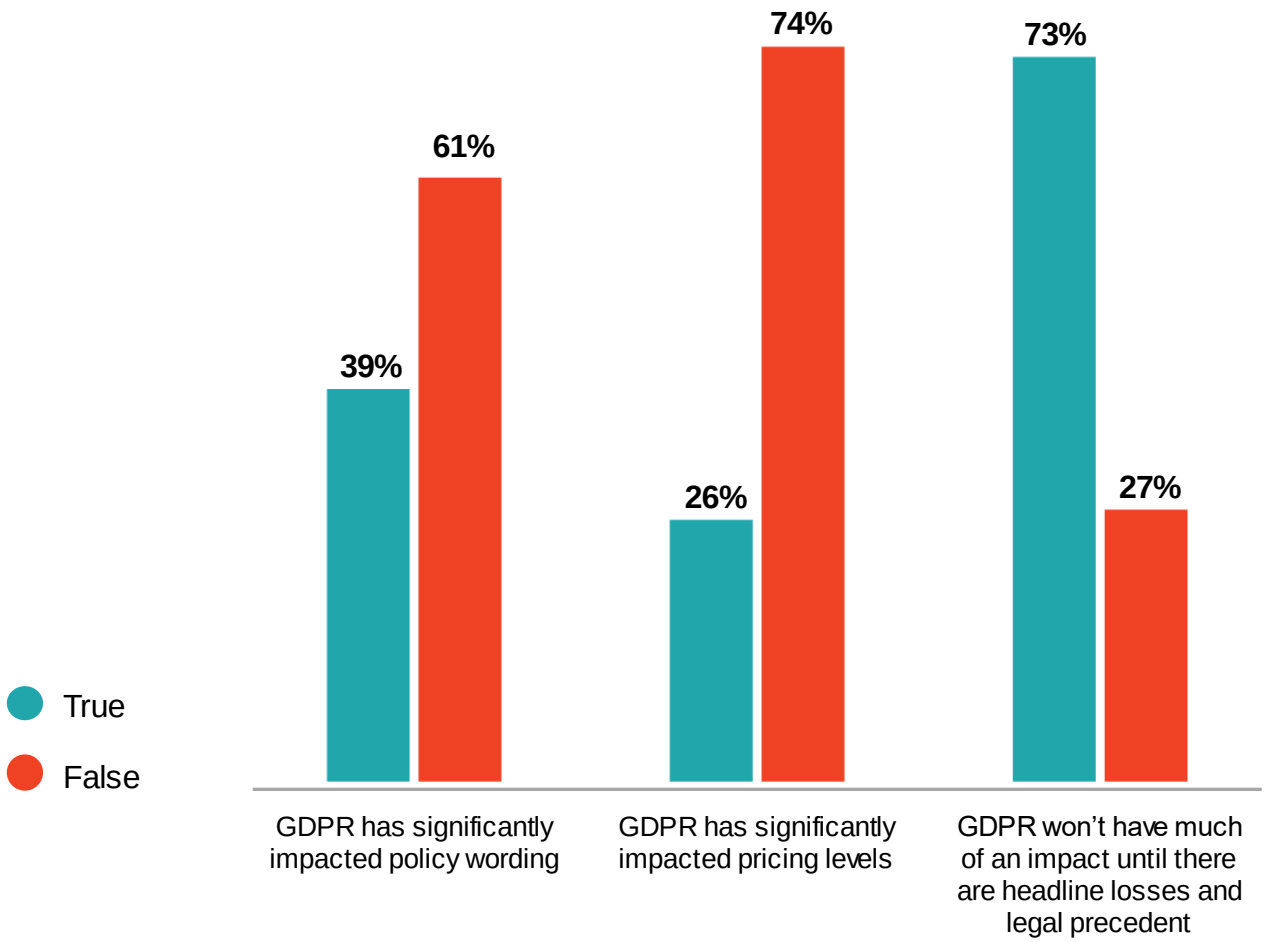
PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

Does your company offer funds transfer fraud loss coverage with the cyber insurance policy?



Similar results to last year despite underwriters preferring the crime policy for this cover (slide 19). Meeting the needs of clients is the likely reason, especially SMEs so **to avoid the need for a separate crime policy**.

What do you think of GDPR? True or False.



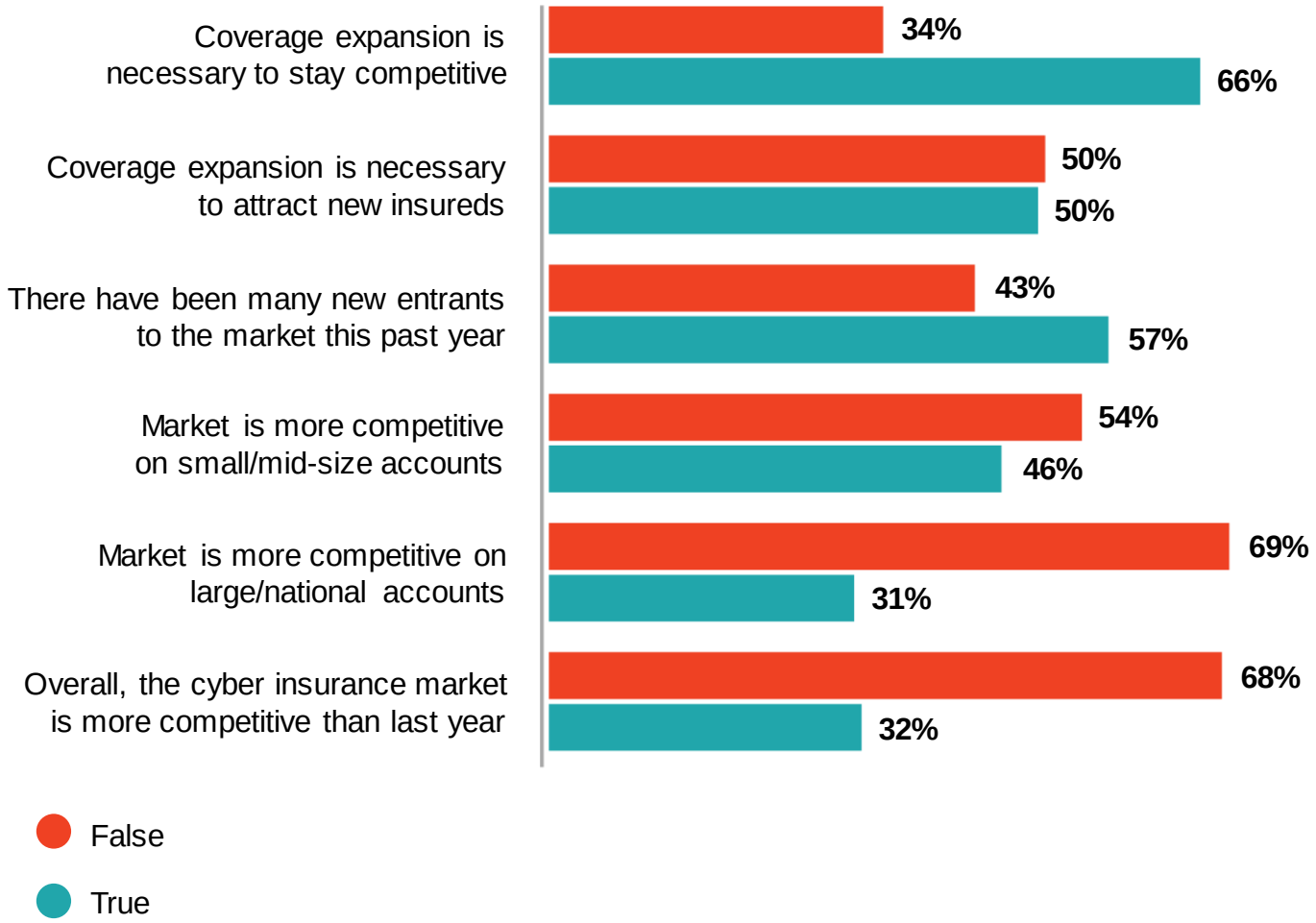
Despite several publicized fines, the **market is not shifting yet because of the GDPR** (see also slides 7 and 9). As the legal landscape is uncertain on the insurability of fines and penalties, the GDPR's impact on the market remains more manageable than was first feared.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

State of the Market

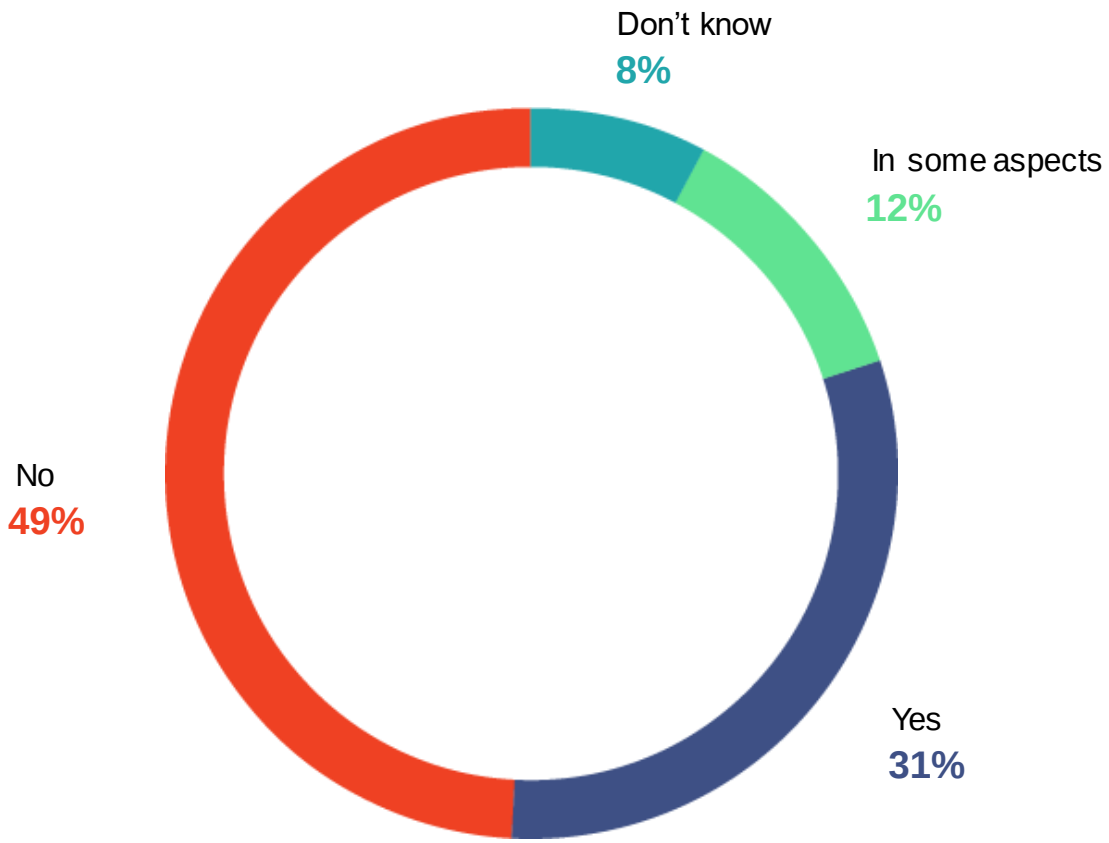
- The hard market has arrived – Most (68%) disagree with the statement that the market has become more competitive, and c.f. last year, a lower percentage of respondents consider that coverage expansion is necessary to attract new insureds or to stay competitive.
- Compared to last year, less brokers (minus 18 percentage points) reported improvements in pricing consistency.
- In contrast, improved coverage consistency continues to be noted by almost 70% of brokers, though comments added that the trend is likely to change as the hard market is introducing disparity.
- Similar to last year, 58% of brokers limit the numbers of carriers they work with for consistency, despite improvements in coverage consistency.
- 90% agree that cyber policies meet the needs of insureds.
- Covid's impact remains uncertain, though the increased risk relating to remote working and increased recognition of the need for cyber insurance were most frequently mentioned by respondents.

Please answer true or false to the following (state of the market).



The hard market has arrived – 68% disagree that the market is more competitive c.f. to only 37% last year. The same trend was noted irrespective of account size. Coverage expansion is also considered less of a must to attract new insureds (minus 8 percentage points) or to remain competitive (minus 13 percentage points).

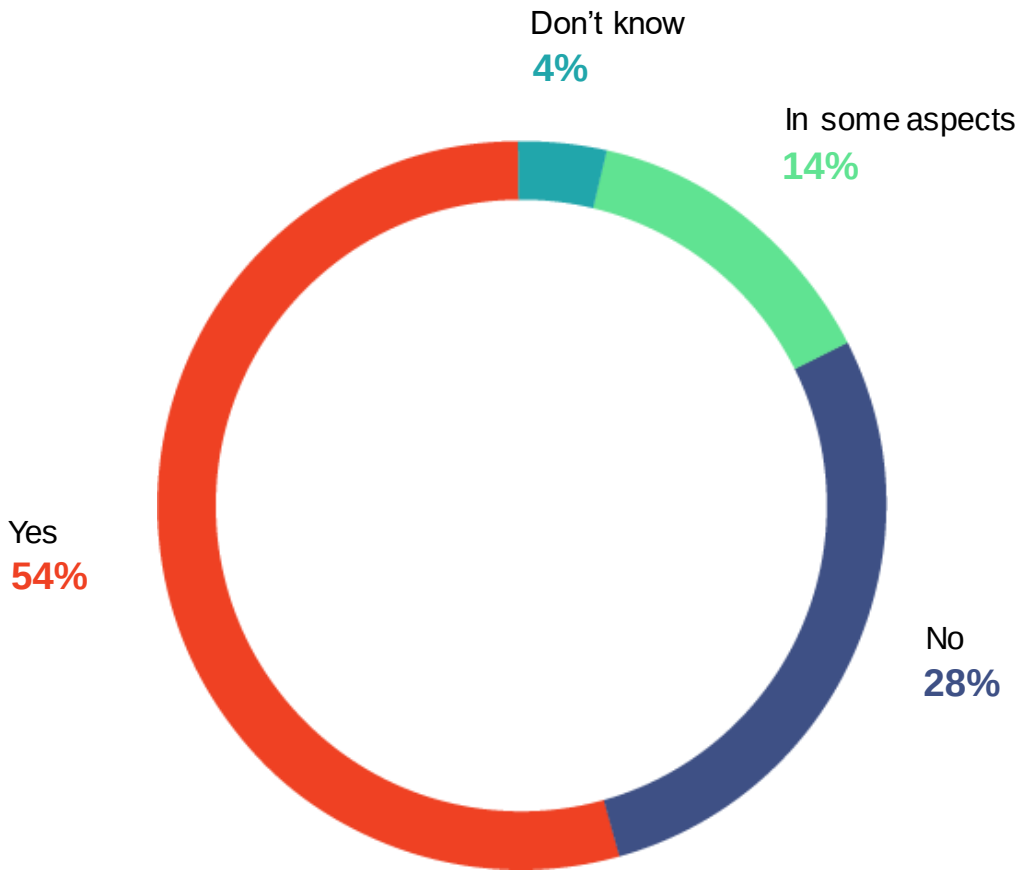
Is cyber insurance pricing becoming more consistent among carriers?



Brokers seeing more consistent pricing, including "In some aspects", fell this year by 18 percentage points. So although the market is evenly split overall, after 2 years of circa 60% reporting consistency improvements, the **market seems to be stabilizing in this respect**. Comments noted that player type makes a difference.

PartnerRe & Advisen.'Cyber Insurance – The Market's View', 2021.

Is cyber insurance coverage becoming more consistent among carriers?



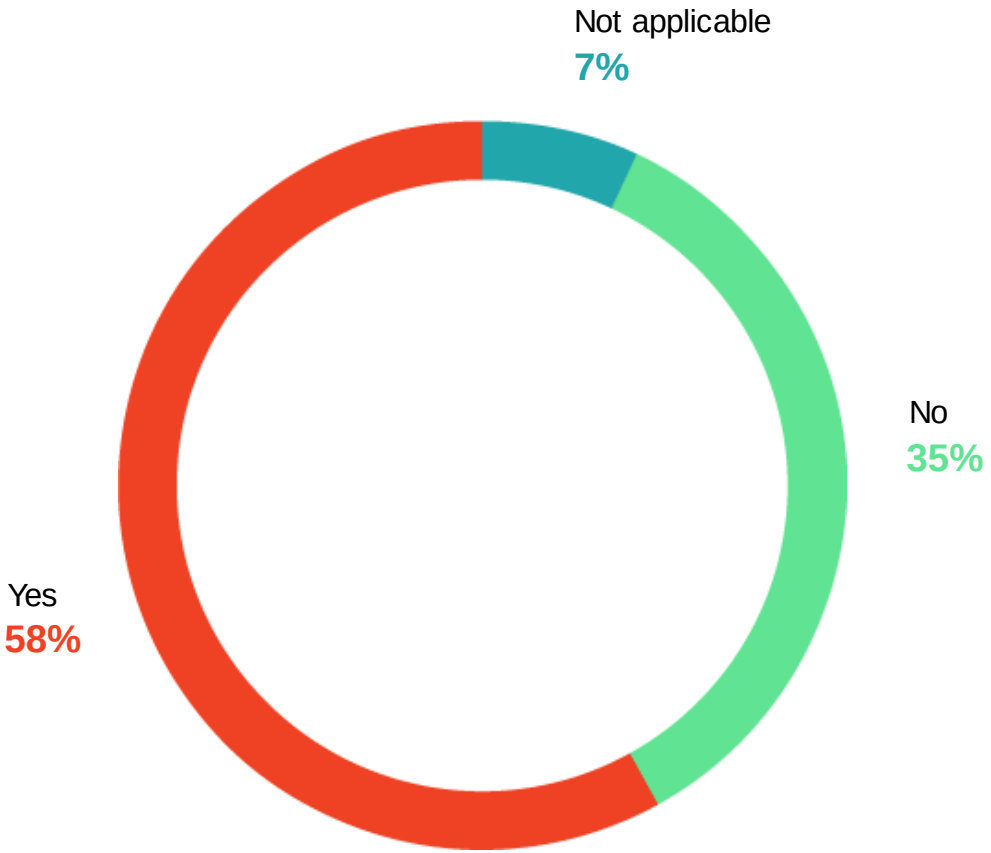
Results are almost identical to last year, with **consistency improvement way ahead overall** at 68%. Interestingly, this is over 20 percentage points higher than for pricing consistency, indicating that risk understanding continues to increase, but that pricing isn't necessarily in line. Comments from the "No" side noted that the hard market is reintroducing coverage disparity, so **next year may see a worsening trend**.

"Coverages overall have stabilized - nothing too crazy being added to policies. Changes in terms and conditions based on UW review/scans can change how the coverage is presented - with larger retentions, sublimits, co-insurance."

"Where we had come to a point where most policies were similar, the hard market is creating disparity again."

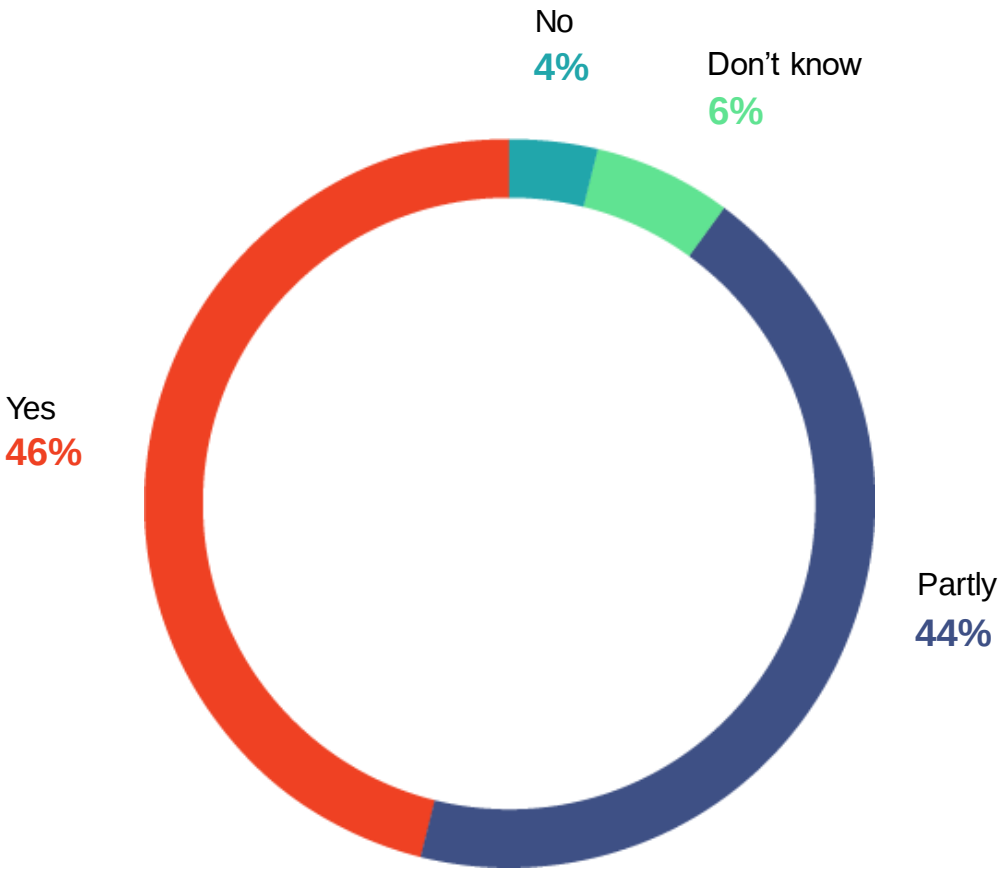
"It remains the wild west from a coverage standpoint. We are spending a lot of time evaluating proposals."

Do you limit the number of carriers that you place primary coverage with due to the wide variety of policies and language?



Very similar results to last year, i.e. the **majority of brokers continue to limit who they work with** – and this despite improved coverage consistency, indicating that trusted relationships have formed.

Do you think cyber insurance policies are meeting the needs of insureds?



Essentially identical to last year, with **90% of all survey respondents saying "Yes" or "Partly".** Many thanks to all respondents for the additional comments given. Notable were comments calling for (1) more focus on risk management for insureds, (2) assistance for brokers to explain the risks, loss examples and covers to insureds, (3) the need for continuous learning, and (4) the absolute critical nature of cyber insurance. In addition, many expressed concerns about the hardening market and restricted access to coverage and capacity.

Do you think cyber insurance policies are meeting the needs of insureds?

"It is going to be constantly evolving as regulation changes and hackers try different ways to commit cyber act. It will be important for carriers and agents to assess position, evolve with the exposure, evolve with regulation, evolve with loss experience."

"Currently there is no capacity available for some of the Asian countries where the vulnerability to cyber risks are great, however, the technology platforms are not necessarily comparable to the European or American markets. This divide needs to be bridged."

"Technology infrastructures are complex, expansive, and managed by a host of interested parties with differing technology awareness. Would like to see policies better address this reality especially as it relates to 3rd-party cloud services."

"We are finally taking a turn towards adequate pricing and collectively underwriting to stronger controls vs the race to the bottom we have been in for a few years. I am optimistic about the future of the market despite the current state of flux, I think we will come out of this stronger by the start of 2022."

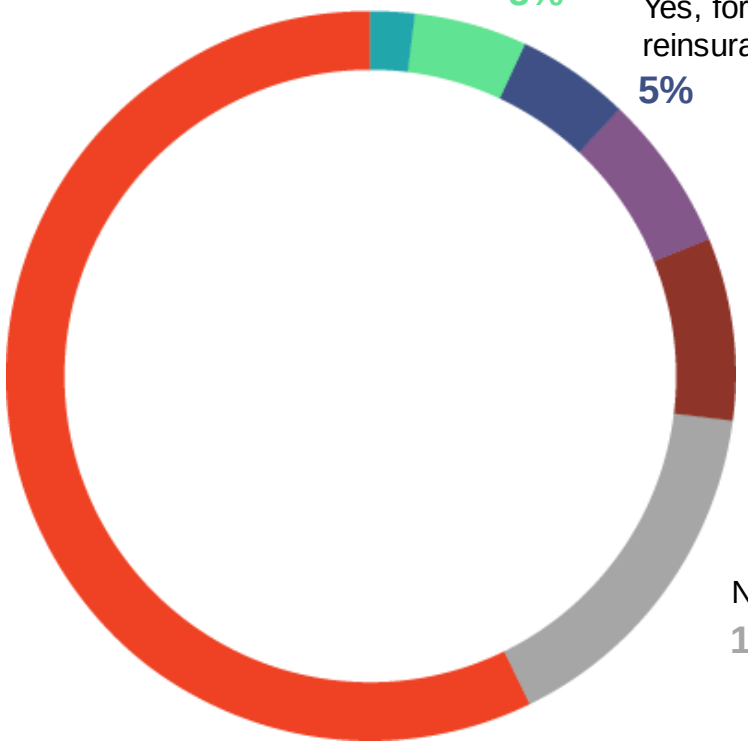
"Insurers are now restricting cover, imposing higher deductibles and lowering the sublimited covers."

"They are [meeting the needs of insureds] today but my concern is that if ransomware losses continue, the reduction in cover for such will get to a point where the policies may no longer have the value to insureds they do today."

"Industry needs to improve on layperson explanations & insurance policies, and providing of numerous claims examples to enable prospective buyers to relate."

"There is little focus on risk management, in my view we should be helping to educate every business in the UK to understand that it is imperative to create a Health & Safety policy around their IT Infrastructure and also to purchase insurance for the ultimate safeguard."

If you place cyber reinsurance, have you seen a notable increase in requests from carriers for any of the following? Please select up to two.



Results were almost identical to last year. Of those placing reinsurance, over half saw an increase in requests for reinsurance, predominantly for proportional and non-proportional covers. **Reinsurance is an increasingly important risk management tool for cyber.**

Please share your views on the impact of the COVID-19 pandemic on the cyber insurance market.

"Clients see more value in cyber insurance as they are relying on their employees being able to connect remotely. They see an increased exposure due to multiple end points that are not within their control."

"It has boosted the demand for cyber cover."

"Wider attack surface and more lax infosec controls from home environment has led to increased loss frequency."

"I do not see a huge impact yet. Cyber market is mostly impacted by Ransomware claims. I haven't seen any concrete evidence yet that the homeworking policies during the pandemic have attributed to an increase in ransomware attacks, even if it would be logical to assume it did have an impact."

Once again, a wide spectrum of responses, indicating that Covid's impact remains uncertain. Overall, the majority report **increased losses associated with remote working and increased recognition of the need for cyber insurance.**

Cyber Insurance

The Market's View

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