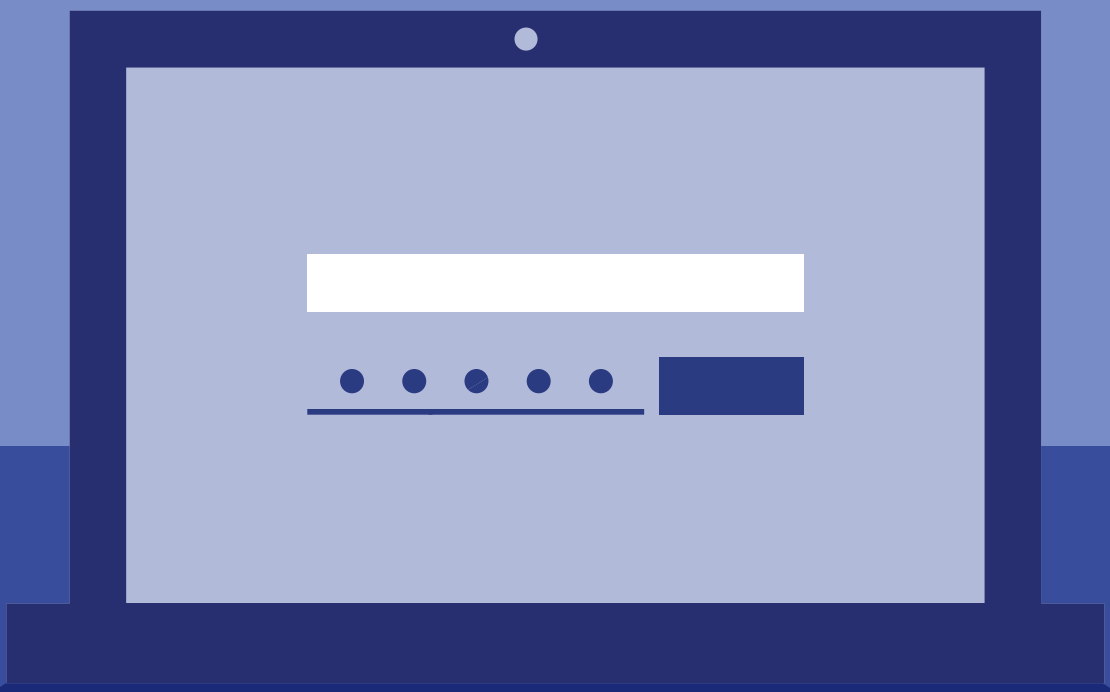
Advisen
Transforming • Insurance℠

PartnerRe



Cyber Insurance – The Market's View.

Key Survey Findings

Coverage understanding has improved – 51% said this is a top–3 sales obstacle. cf. 63% last year

Rates have increased 5-10%, report many brokers

Board/senior management are driving more cyber sales – now in 3rd place cf. 5th last year

Cyber-related business interruption still most sought after cyber coverage – 68% put this in their top 3.

60% agree, **insureds frequently request higher limits**

Majority of brokers report **increased market consistency** in pricing (61%) and coverage (72%)

77% agree, **still no significant impact on pricing from GDPR**

60% agree, **funds transfer fraud loss/ social engineering belongs with 'Crime'**

64% of brokers still limit number of carriers they work with for consistency

Use of outside vendors for aspects of aggregation management rises from 29% to 40%

Agree, **aggregation management impacts underwriting and pricing decisions –** up from 73% last year

Of **underwriters are concerned by non-affirmative cyber** in specialty property

Advisen Transforming • Insurance | PartnerRe

Survey Information

A global survey

We are pleased to present the results of our comprehensive global survey of the cyber insurance market, a joint venture by **PartnerRe and Advisen**, now carried out for the seventh year running.

The survey took place during the second quarter of 2020, with 260 cyber insurance brokers and 190 cyber underwriters from around the world sharing their observations and views on the latest trends and developments.

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

With commentary and interpretation throughout from PartnerRe's cyber risk experts

Andrew Laing
Cyber P&C Worldwide
andrew.laing@partnerre.com

Ho-Tay Ma
Cyber P&C North America
ho-tay.ma@partnerre.com

Christopher McEvoy
Cyber P&C Europe
christopher.mcevoy@partnerre.com

PartnerRe

We are a privately-owned, leading global reinsurer with a strong balance sheet and the scale and expertise to meet our clients' needs across multiple 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 for all types of cyber risk.

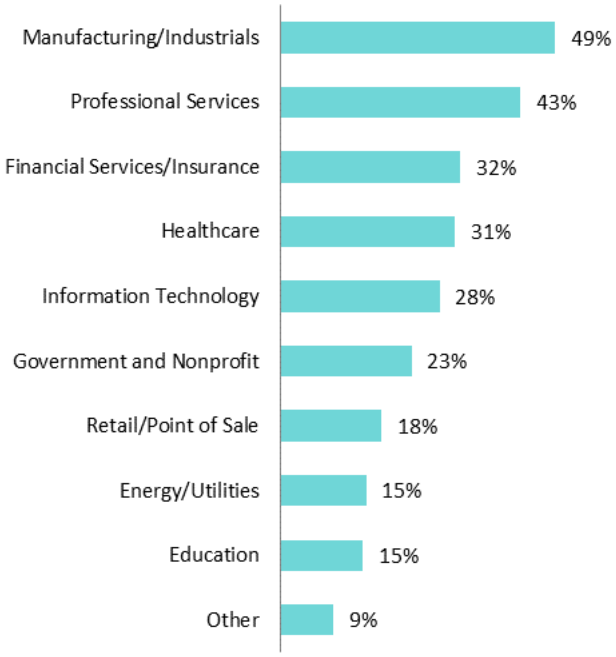
Find out more about our cyber risk solutions: partnerre.com/risk-solutions/cyber-risk

For more information about this survey or to request to reproduce material herein, please contact the editor (Dr. Sara Thomas; sara.thomas@partnerre.com).

Sales Motivations

New-to-market buyers are familiar faces

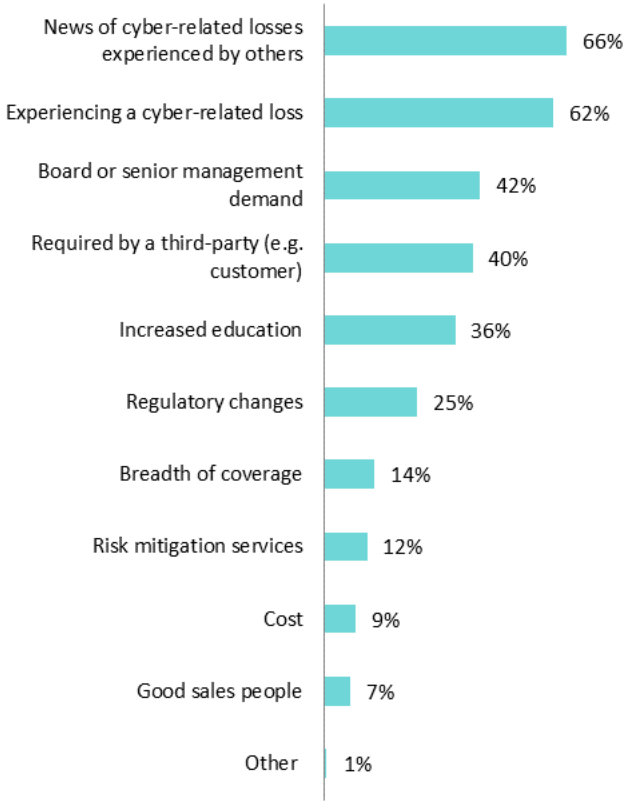
Q What industries brought the most new-to-market buyers of standalone cyber insurance (including those switching from endorsements)? Please select top three:



Continuing a trend that began last year, 'Manufacturing/industrial' generated the most new-to-market buyers to the standalone cyber market, with nearly half of our survey respondents identifying the sector among their top three. Interestingly, 'Healthcare', which took the top spot in the 2018 survey, dropped to fourth place, suggesting higher levels of cyber insurance penetration have now been reached in this industry known as a frequent target for data breach.

Increasing demand from boards and senior management

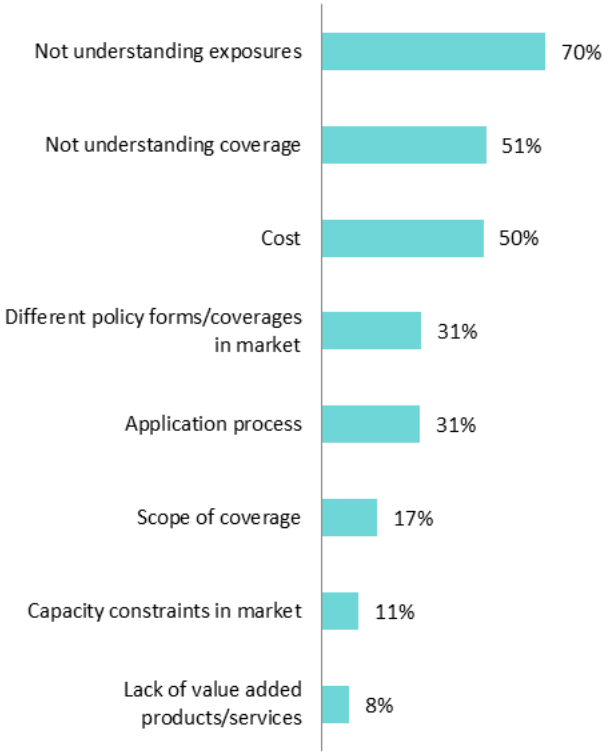
Q What do you see as the top driver(s) of new/increased cyber insurance sales? Please select top three:



Cyber insurance buyers clearly take lessons from their peers – 'News of cyber-related losses experienced by others' and 'Experiencing a cyber-related loss', continue from last year as the two most common drivers of cyber insurance sales for brokers and underwriters. 'Board or senior management demand' is on the rise, however, signaling a new trend of increasing awareness of the risks faced by organizations. 'Required by a third-party (e.g. customer)' has maintained its position among the top four drivers as organizations continue to place a high priority on the cybersecurity posture of their business partners.

Cost increasingly an obstacle to sales

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



The top three obstacles to selling and writing cyber insurance remain, as in past years: 'Not understanding exposures', 'Not understanding coverage' and 'Cost'. On a positive note, 'Not understanding coverage' has reduced its percentage point lead year-over-year as buyers have become more familiar with the coverage options in the market; over the last year, for example, this category dropped from 63% to 51% and actually came in third to 'Cost' for underwriters. The fact that 'Cost' has held, and for underwriters strengthened, its position as a top three obstacle, is a trend that tracks with the survey finding that the market is becoming less competitive (see section, State of the Market). As one respondent noted, "Market conditions of all other lines [are] driving overall costs and new cyber is not in the budget."

The continued dominance of 'Not understanding exposures' was reflected in comments from respondents pointing to struggles that some organizations have quantifying and conveying their cyber risk exposures. Several brokers, for example, commented that clients have yet to understand the risks facing their organizations, and that even now some still have the "'It will never happen to me' mentality."

Giving a deeper insight into lost potential sales, underwriters expressed some frustration at not being provided with enough underwriting information, with one respondent saying, "Often times brokers are not willing to work with carriers who ask for 'too much' info."

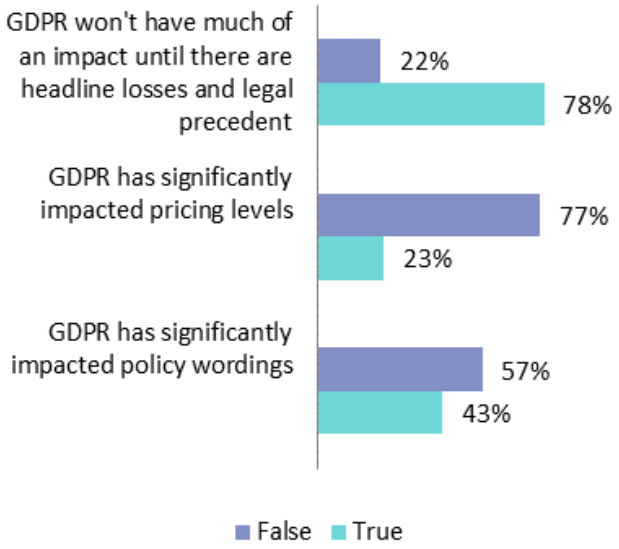
Linked to selection of the sales obstacle category 'Different policy forms/coverages in market', several brokers respondents commented that "lack of standardized terminology" and "inconsistency in policy language" create barriers to entry for many buyers. Underwriters equally saw this category as an issue for sales. On a positive note, coverage consistency is continuing to increase, as shown further on in the survey (see section, State of the Market), so this issue is likely to improve.

Regulatory impact yet to materialize

Q Which regulations do you think will have the largest impact on cyber sales? Please select one.

Respondents predicted that the California Consumer Privacy Act (CCPA) will have as much of an impact (both were close to 40%) on cyber sales as the European Union's General Data Protection Regulation (GDPR). The Illinois Biometric Information Privacy Act (BIPA) wasn't viewed by many as having a significant impact (13%). One underwriter responded, "All of the above – whichever has a large penalty applied first". As the following question shows, it's still early days and uncertainty around application remains.

Q What do you think of GDPR? True or False.



In results that were almost identical to last year, most respondents agreed that the GDPR will not have a major impact until there are headline losses and legal precedent. Only a quarter saw any impact so far on pricing levels, and less than half felt that it has impacted policy wordings.

Overall, all regulations are expected to have an impact, particularly the headline regulations CCPA and GDPR, but enforcement will be the decisive factor.

Expert Comment

"With network breaches increasingly headline news, it's understandable that these prompt organizations to take steps to reduce their own potential exposure to similar events. Cyber insurance products are rightly promoted as an option to be explored to mitigate this concern. Conversely, a firm's own experience of a network breach will provide first-hand experience of the detrimental impact these events can have, driving a desire to purchase dedicated products designed for new, unpredictable exposures. The survey also identifies board and senior management demand as an increasingly significant driver of sales - this goes hand-in-hand with regulatory change and education in generating policy sales traction. New and updated regulation continues to place additional and wide-ranging requirements on senior management to securely and responsibly manage and store data, and to act swiftly to inform data subjects should the worst occur. Given the severe potential impact, it's unsurprising to see board and senior management seeking out products that are designed to respond efficiently and quickly to breach events.

"In-roads being made to improve understanding of cyber coverage are a positive sign for the industry – dedicated brokers being a key factor in this achievement. Looping back to regulation, similar in-roads into understanding exposures – still the leading obstacle to sales - are likely hampered by the complexity of regulation and its lack of enforcements to-date."

Christopher McEvoy
P&C EMEA, Senior Underwriter,
Specialty Casualty, PartnerRe

Coverage Requests

Endorsements are falling out of fashion

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

Tellingly, the number of respondents answering this question was notably low, with many commenting that the question was "not applicable" to them.

Several underwriters specifically commented here that their companies do not offer cyber endorsements, and many brokers said they placed none, finding insurers "reluctant" to offer them. One stated, "I see a clear tendency for standalone", while another said, "Endorsements are not worth it."

Of those that do seek this coverage type, most respondents put 'Professional services' in their top three new-to-market buyer industries (39%), followed by 'Manufacturing/industrials' (26%); these are the same two leading buyer categories as for standalone cyber insurance (see first question in this section). A few commented that smaller, more "price-conscious" businesses might look to endorsements, but as one respondent noted, "The cyber market has been so cheap that small businesses can buy a policy once they realize the expanded coverages." For more on market competitiveness for SME accounts, see section, State of the Market.

Q **If you have you seen cyber business switch from endorsements to standalone policies in 2020, what is the main reason(s)? Please select top three:**

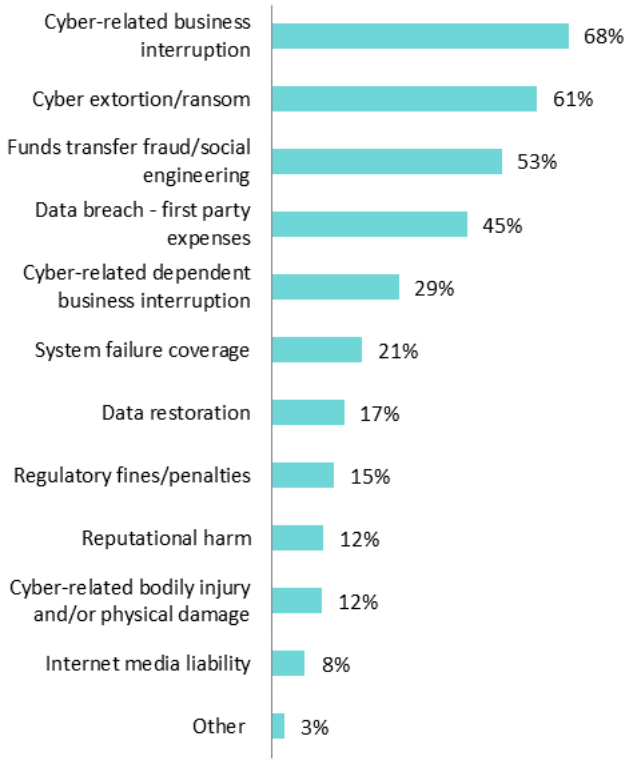
Leading by a clear 21 percentage points, most respondents say that their clients switch from endorsements to standalone because they are 'Looking for dedicated limit for cyber coverage' (59%). This offers more evidence of a maturing cyber insurance market – buyers want to transfer more risk and the industry is meeting that demand. Also among the most common reasons for switching were, in descending order, 'Looking for more limit' (38%), 'Looking for other areas of expanded coverage' (37%), 'Looking for expanded business interruption/ contingent business interruption' (33%), and 'Looking for more clarity of coverage' (30%). One broker commented, "Carrier took away cyber endorsement feeling clients should be buying dedicated policies."

Commenting further on cyber endorsements, underwriters reported feeling that endorsements in traditional lines may blur the line too much, creating potentially problematic coverage overlaps. A few respondents also cited some mixed results on the part of traditional lines to expressly provide coverage for cyber-related losses. One underwriter said, "We are seeing 'Cyber' extensions show up on all sorts of coverages where it truly does not belong - Fiduciary, D&O, etc."

One broker's comment summed up many respondents' sentiments: "Any company would benefit from standalone coverage because it is specifically designed for the risk. Creating an endorsement on a property form does not necessarily provide the best coverage."

Cyber-related business interruption increases lead as most-requested coverage

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

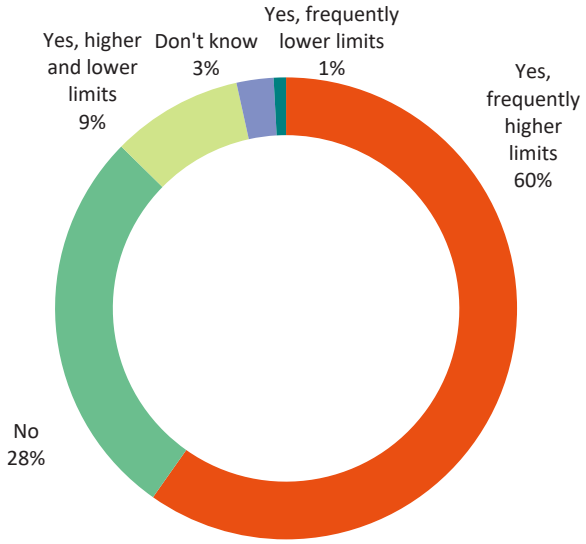


'Cyber-related business interruption' remains (now for the third year running) the most-requested coverage, creeping up a further 8 percentage points in 2020.

'Cyber extortion/ransom' has steadily moved up, now just eclipsing last year's number-two coverage, 'Funds transfer fraud/social engineering', which has dropped to third place. This makes sense, given the fact that ransomware attacks increased in prevalence over the last year, causing both financial damage and business disruption for victimized organizations. News reports of ransomware incidents have become a near-daily occurrence and are helping to drive awareness of the risks to all businesses.

Higher limits still sought, though interest may have plateaued

Q Are your renewal insureds frequently requesting different cyber insurance limits?



As cyber risks escalate, the clear majority of brokers and underwriter respondents report frequent interest in higher limits at renewal. The 28% 'No' result to this question is also of interest; it may indicate that insureds are reaching limit adequacy - or, for higher limits, that many buyers find these carry too high a price in today's market, harkening back to 'Cost' as a key obstacle to sales.

In comments, some underwriters partly attributed interest in higher limits to "genuine recognition" of the exposures, while several brokers noted that higher limits are still a "hard sell" and that many buyers need to experience a loss before realizing that they need more coverage.

Expert Comment

"After years of expansion in coverage terms, 2020 is seeing a significant slowdown as the industry digests the coverages offered in years past. Ransomware, for example, was first offered over a decade ago, almost as a thrown in, but is now a significant loss component of many cyber portfolios. The industry is reflecting on coverage expansion's impact on individual portfolios, unit performance and enterprise risk management. We see this in the increased use of risk management tools, portfolio modeling and, in an indirect way, in the consistent feedback in this survey that 'Not understanding coverage' remains a major obstacle to writing cyber. This response can only be said so many times before underwriting management and broker e&o exposure is triggered – hence PartnerRe has long offered quota share and aggregate stop loss solutions to insurers looking for downside protection."

Ho-Tay Ma
North America, P&C VP, Senior Underwriter, Cyber Liability, PartnerRe

Coverage Overlaps & Questions

Coverage overlap continues, but at a slowing pace

Q Coverage overlap between cyber and other policies has?:

The results show a close race on whether coverage overlaps have 'Increased' (31%), 'Decreased' (31%), or 'Stayed the same' (29%). The percentage of respondents who feel that overlaps have increased has continued to drop over the last three years - down to 31% this year from 36% in 2019 and 51% in 2018 - this signals success on the part of the industry to achieve as much coverage clarity as possible, and is in line with the continuing move to standalone cyber and dedicated limits.

Comments indicate that efforts to address silent cyber exposures (see following question) will soon lead to a more significant reduction in overlap.

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

Silent cyber issues remain a chief cause of concern for underwriters, according to the survey, with 65% of underwriters saying that non-affirmative cyber cover on specialty property risks worries them. One underwriter said that silent cyber issues "can cause serious surprises in manuscript all risk policies that have been in the market for a long time". Several commenters pointed to ongoing work on wordings in their companies and in the industry toward "eradicating silent cyber".

Respondents expressed hope that the UK Prudential Regulation Authority and Lloyd's of London affirmative cyber initiatives will soon ease coverage uncertainties.

"Traditional insurers are scaling back their otherwise covered causes of loss when a cyber event is part of a chain of causation (silent cyber exposure)," said one broker. "Insureds are increasingly looking to cyber insurers to solve these issues."

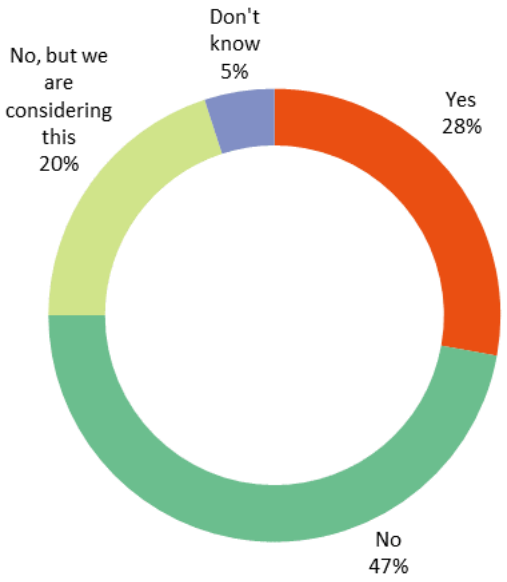
Split views on cyber-related physical damage

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

We annually ask where cyber-related physical damage should be covered and, according to the survey, this remains an unsettled area between brokers and underwriters: most underwriters (61%) plumped for the traditional property policy, while most brokers (51%) chose dedicated cyber.

Despite the difference in answers, many comments reflect converging views – brokers agreed that it depends on the risk and the trigger, some calling it a "grey area". Multiple respondents from both sides of the market said they feel that property and cyber underwriters should collaborate more to create a separate product or provide some coverage on both policies. Underwriters cited the difference in underwriting practices between cyber and property, as well as the lack of capacity in the cyber market to provide the right limits for cyber-related physical damage. One respondent commented, "I can see the argument to place it under the cyber, but in order for it to become industry standard to be covered under cyber policies, cyber premiums/rates must increase", while another added, "[Physical damage] within cyber policies can be useful, but for sophisticated property risks such as energy plants, the cyber market doesn't have nearly enough capacity to cover some of the significant sums insured … so property market needs to embrace this exposure." Other comments from underwriters spoke to the need to tailor coverage to insureds' specific exposures and causes of loss.

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



Perhaps not surprisingly given the answer to the previous question, the majority of underwriters said that their company's cyber product does not cover cyber-related bodily injury and/or physical damage. This is an increase from last year's 39%, signaling a clear market shift. However, 28% do include this, and a further 20% are considering it, so an openness to all solutions seems to be holding. Comments from underwriters indicated that some will make exceptions based on broker requests or on an excess coverage basis.

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

In line with the response to our earlier question on most-requested coverages, cyber insurance buyers in any case do not appear to be pressuring the industry for cyber-related bodily-injury and/or physical damage coverage; relatively few respondents said that they receive frequent requests for cyber-related physical damage coverage. The majority said they only 'Sometimes' (51%) or 'Rarely/Never' (36%) see interest in this coverage. This may begin to change though, since 'Sometimes' has increased as a response since last year (now 51%, compared to last year's 40%) at the expense of 'Rarely/Never' (now 36%, compared to last year's 50%).

Social engineering belongs with crime

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

Unlike with physical damage, there is almost universal agreement in the industry as to whether funds transfer fraud loss due to social engineering should be covered under 'Crime' or 'Cyber' – the majority (73%) of underwriters voted for 'Crime', and the majority (51%) of brokers agreed.

Comments from respondents, however, indicated more nuance to these answers. Underwriters and brokers see room for a blend between the two coverages, or two policies that work in concert with each other, with crime picking up the financial loss and cyber stepping in to provide forensic investigation. Respondents on both sides recognize that the details of individual events matter in guiding which policy responds. Brokers also cited the availability of higher limits under crime policies or a combination of the two markets.

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

In terms of availability, 80% of underwriters say they either 'Always' or 'Sometimes' offer funds transfer fraud loss coverage on their cyber policies, an increase from last year's 68%. This is interesting as this isn't the market's preferred choice but is again likely a result of the market's willingness to be flexible.

Expert Comment

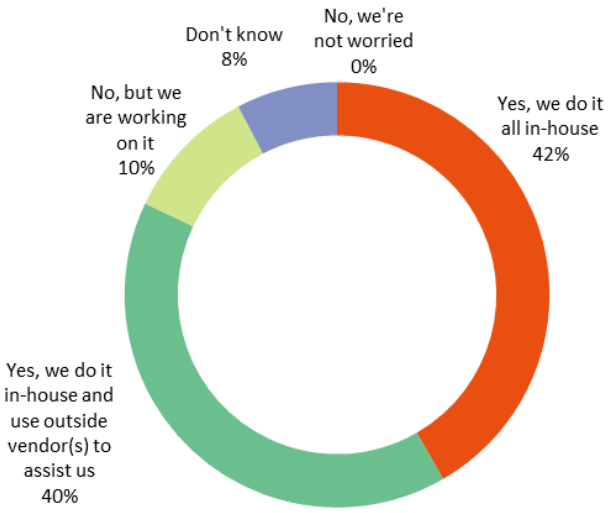
"The industry is beginning to see the initial feedback on efforts by Lloyd's and several leading cyber carriers mandating the identification, classification and, most importantly, affirmation/exclusion of cyber coverage on policies. Removing coverage ambiguity requires seeing the perspective of many stakeholders to drive a coherent strategy, which may mean reduced coverage and/or higher rates. Maintaining the status quo is easier, one factor behind why polling remains varied on where coverages such as bodily injury, property damage and crime should be covered. I'm hopeful for the future as knowledge expands on coverages, loss costs of bodily injury/property damage claims, and rating mechanisms used by non-cyber policies. PartnerRe believes in having this broad and flexible perspective, which is why our cyber team is comprised of experts in cyber liability who also have many years of underwriting experience in property, casualty and catastrophe loss portfolios."

Ho-Tay Ma
North America, P&C VP, Senior Underwriter, Cyber Liability, PartnerRe

Risk Aggregation

Increasing emphasis on risk aggregation and use of external vendors

Q Is aggregation actively managed by your company?



Our annual questions for underwriters on the accumulation of risk showed a continuing trend toward using outside (third-party) vendors for help in actively managing aggregation - 40% now manage it in-house and use outside vendors, up from 29% in 2019 and 16% in 2018. This increase is not at the expense of 'Yes, we do it all in-house', so the indication is a growing maturity around the need to manage cyber risk aggregation and of areas where outside perspectives can be useful.

Q Does aggregation management impact your underwriting or pricing decisions?

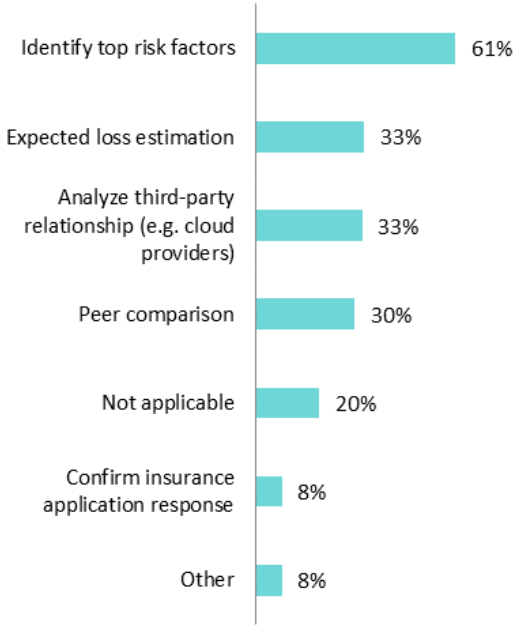
Aggregation management is also having more of an impact on underwriting and pricing - an overwhelming majority of underwriters (90%) said it 'Always' or 'Sometimes' affects their decisions. This is a significant jump up from 73% in 2019 and confirms a trend we noticed last year. An improving grip on aggregation could also help to explain why cost remains a key consideration for buyers.

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

In this new survey question, most underwriters (44%) answered 'Always, to some extent'. Another 11% answered 'Always, to a great extent'. Within comments, underwriters indicated that they find vendors useful for added insight into complex risks and specific industries, as well as to underwrite higher limits more effectively.

Comments also identified reasons why some underwriters don't see value in third-party vendors in the underwriting process. One underwriter said, "We don't believe there is a third-party solution that can add value and materially change our views in the underwriting process", while another commented, "They are too expensive and are not able to give you what you need", another cited that they can be "unreliable".

Q If you use third-party vendors, what are your primary uses of vendor products during the underwriting process? Please select up to three:



This new question highlights the main usage in underwriting of third-party vendors; usage is varied but using vendors to 'Identify top risk factors' clearly tops the chart.

Q Do you analyze the systemic nature of the exposure?

With insureds requesting higher limits and pressures on expanded coverage (see following question), it should be heartening to learn that nearly all (91%) of underwriters said they analyze the systemic nature of cyber risk. Respondents said they do this by modeling systemic cyber event scenarios, examining their insureds' interconnectedness and cyber controls, and by attempting to diversify their books of business.

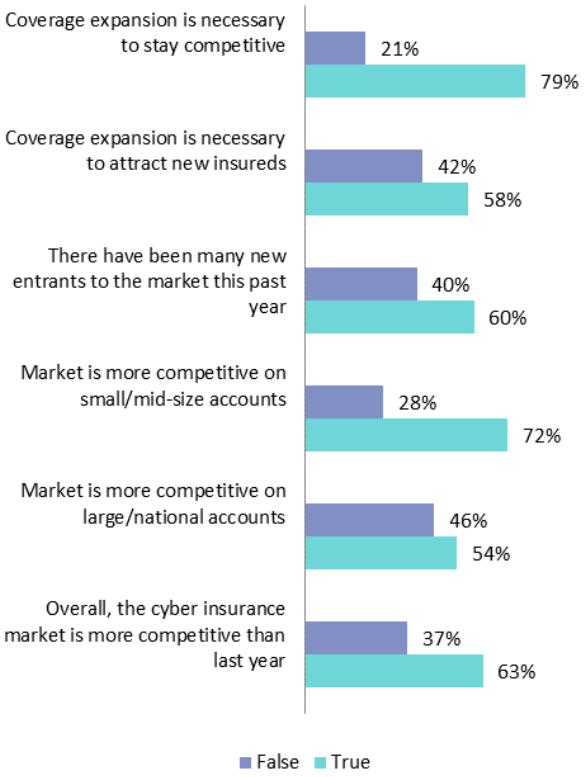
Expert Comment

"Risk aggregation tools for cyber are increasingly vital in understanding the interconnected nature of insureds, and we are pleased that most surveyed underwriters are already actively managing their aggregations. Cyber perils present a unique aggregation profile, where for example the country and size of a company may be less important than the software version or cloud provider they are using. Capturing this crucial firmographic data at a useable resolution and for a reasonable cost will remain an industry challenge for some time. But more importantly, using this data intelligently will differentiate insurers in the long term. Understanding risk is not the only solution however; mitigating this risk through reinsurance or other risk transfer mechanisms will be a key industry solution, whether for individual accumulations or concerns over events that could send ripples through the industry."

Andrew Laing
Head of Cyber & Emerging Risks, PartnerRe

State of the Market

Competition is leveling off and rates are on the up



The last two years of this survey have reflected an increasingly competitive marketplace, with new entrants and lower prices, along with some concerns that pricing was too low. Again this year, the majority see a more competitive market, but in a notable shift, the gap is closing; this year, 63% of respondents felt that the market has become more competitive, compared to 86% and 90% respectively in 2019 and 2018.

While respondents see more competition across all business sizes, increased competition is reported substantially more for small/mid-size accounts than for large/national accounts.

Asked whether or not coverage expansion is necessary to stay competitive and attract new insureds, the majority answered yes to both questions. There was, however, lower agreement on this from underwriters, especially regarding coverage expansion to attract new insureds (only 43% agreed, compared to 68% of brokers).

Q **Please comment on average risk-adjusted rate changes over the last 12 months.**

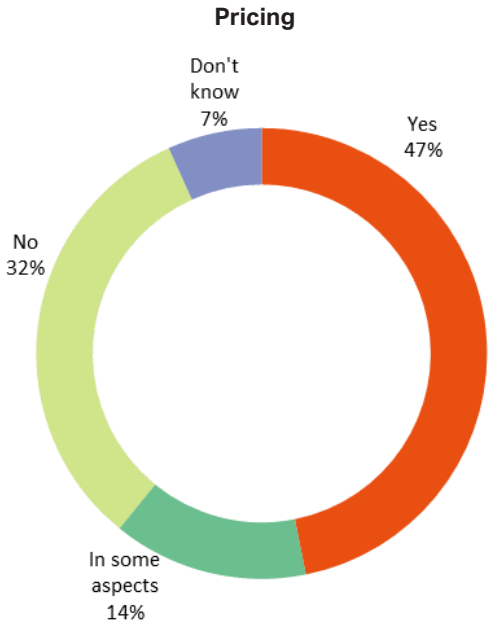
As the market begins its slow-down in competitive expansion, comes a trend toward higher pricing. Asked to comment on the average risk-adjusted rate change over the last 12 months, most brokers indicated rate increases of between 5% and 10%, citing higher claim frequency and insurers' improved ability to evaluate the risk. As one broker commented, "Seeing rate increases of 5% to 10% depending on carrier, but reasons have same nexus: Increase in ransomware claims driving claim costs."

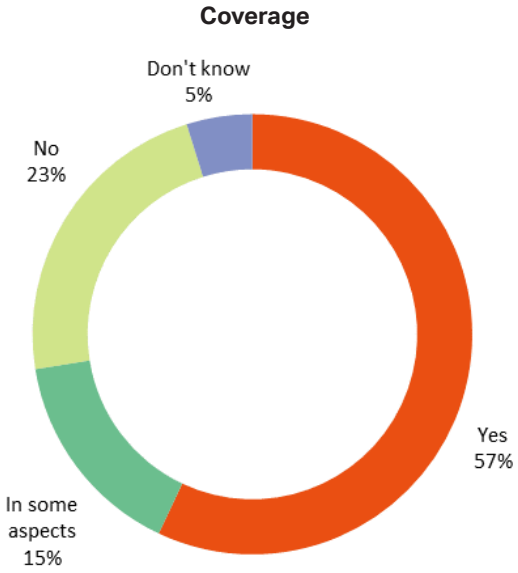
Underwriters' responses varied from flat to +30%. Comments reflected a clear need for rate due to ransomware losses, with one underwriter commenting that increases were "Not as much as we would like." Others expressed concern that price hikes would cause them to lose business, with comments such as "Rate change is a challenge in this market and we will lose deals because of this" and "We are basically pushing rates 10% avg. Mostly, due to competition, we end up with lower increases."

For the first time we asked brokers who place cyber reinsurance if they have observed any notable increase in requests for various reinsurance structures or increased cessions on existing reinsurance programs. Approximately half said they had, with similar percentages across proportional and non-proportional treaties including aggregate placements, specific non-affirmative covers and higher cessions.

Market consistency continues to improve

Q Is cyber insurance pricing and coverage becoming more consistent among carriers?





In this question posed only to brokers, the majority responded that cyber insurance pricing and coverage are becoming more consistent, either in general or in part. These results were virtually identical to last year, suggesting the continued and strong trend of a maturing market.

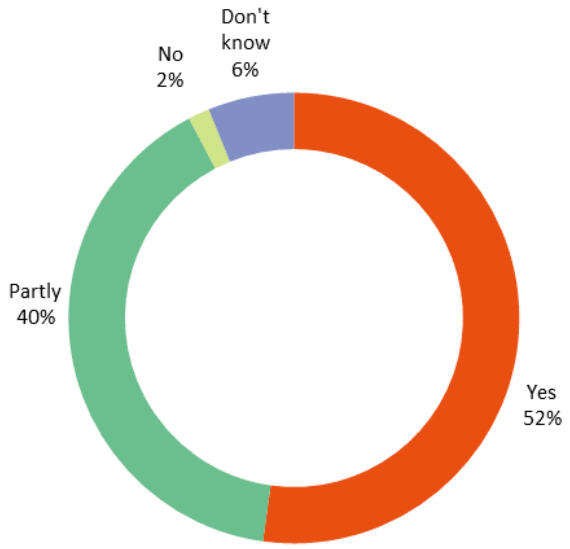
In comments, brokers pointed to the use of risk modeling and more experience in underwriting as reasons for pricing consistency. A third of respondents, however, did not see an increase in pricing consistency. In comments, several noted a divide in the market, with more established underwriters declining to compete with InsureTechs on price. Others noted that even though basic coverages from the "big players" show more standardization, there are other provisions and newer carriers where terminology varies. As one broker noted, "Yes, but there still is truly no standard policy language."

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

Consistency continues to affect where brokers place business – as in past years, most (64%) say that consistency prompts them to limit the number of carriers they use.

Market meets the needs of insureds

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



In the view of most respondents, cyber insurance policies meet the needs of insureds, entirely or in part. The views expressed speak to the evolving nature of the market and its ability to shift as quickly as possible to market demands. Respondents praised the "nimble and innovative" market and said that "For the price, cyber is a great deal and more insureds should be buying it".

That 40% selected 'Partly', shows room for improvement. Many respondents shared their ideas. Several mentioned the need to make policies "more user-friendly" and highlighted areas where coverage needs to be stepped up in order to be truly effective, including business interruption and pre-breach services for smaller businesses.

One respondent said, "We need greater uniformity in coverage across the market to make cyber more accessible to risk managers and clients. The information gathering requirements imposed on insureds is lengthy and laborious and can put off many risk managers. The insurance market needs to work hard on how they can reduce this burden for insureds."

One respondent felt the industry may be taking on more than it can handle, "The Cyber market is not yet ready to be the answer to all cyber exposures in the insurance market nor - on its own - does it have the expertise to be so. The cyber market should focus on its core product and expertise, maintain the relevance of that product and maximise penetration for it whilst staying profitable."

Another commented, "The disparity in policy language from carrier to carrier makes [cyber] coverage difficult for clients to understand and agents to sell. It makes the clients wonder what they are buying. We need some consistency in at least basic terminology."

The replies may be best summed up by one respondent's comment: "Considering the ever-changing world, cyber policies are a work in progress."

Wide-ranging views on the impact of COVID-19

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

The wide spectrum of answers to this question shows how COVID-19's impact on cyber remains uncertain.

Several expressed concerns, such as that we are in the "quiet before the storm", and that "there are breaches which have yet to be discovered."

Work-from-home was often cited as likely to increase the exposure/losses as cybercriminals take advantage of the disruption. For example, "Heightened awareness of the risks posed by a largely remote workforce may encourage premium growth, but those same risks will likely drive further losses."

Other respondents felt cyber insurance could fall from the spotlight as organizations wrestle with reduced revenues from COVID-19, but that it would rebound in the long term. Similarly, several noted that their customers "are too busy right now to even talk about it" as they focus on survival, particularly SMEs.

One respondent added, "In general, this pandemic will test the cyber culture organizations have (or haven't) created. Those that have been proactive to considering the multifaceted cyber risk exposures will [be] better prepared to handle the remote demands that are being thrust upon them. Those that haven't, are more likely to stumble along the way, leading to a great likelihood to experience a breach."

Expert Comment

"2020 has marked a turning point for many in the cyber market. With ransomware losses helping to drive increasing attritional loss ratios and growing concern about tail risk, we are encouraged by the actions the market is taking in this shifting environment. Investments in analytics, clarification of non-affirmative cyber coverage, slowing of coverage expansions, and rate increases will all greatly benefit the industry over the long term. In addition, brokers are continuously bringing new buyers to the market, increasing the diversity of insureds. However, the changes to date may not be enough to stem the increasing loss trends the cyber market has faced recently. Many of our clients report projected rate increases in 2021 similar to those seen in 2020. Whether this will be sufficient, bearing in mind that increases are not enough this year to stop creeping loss ratios and that new issues can arise, needs consideration."

Andrew Laing
Head of Cyber & Emerging Risks, PartnerRe

Disclaimer: