Advisen
Transforming • Insurance℠

PartnerRe

2018 Survey of Cyber Insurance Market Trends

PartnerRe & Advisen

For the fifth 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

For this year's survey, we queried 270 brokers and 70 underwriters from around the globe on their observations of the cyber insurance marketplace. Respondents were primarily from North America, as were most of their insureds, but there was also a representative international presence.

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.

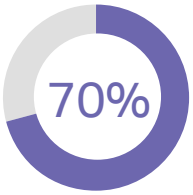
This report summarizes the survey's findings. However, we received many more valuable insights than can be incorporated in this report. If you would like to view all of the survey's graphed results, please go to: **https://partnerre.com/opinions_research/2018-survey-of-cyber-insurance-market-trends/**

Survey Highlights

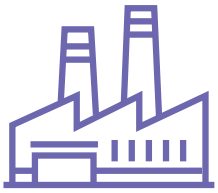
- The shift from endorsement to standalone cyber policies continues as insureds seek dedicated limits, higher limits, and expanded coverage, emphasizing the need for a separate cyber insurance market.
- 'News of cyber-related losses experienced by others' and 'experiencing a cyber-related loss' held onto the top two spots as the main drivers of cyber product sales.
- Buying cyber coverage because it was 'required by a third party' moved up from fourth to third place, despite stiff competition from the new category of 'regulatory changes'.
- There has been a healthy take-up of coverage by SMBs and by less traditional buyer sectors including manufacturing, which together with healthcare and professional services, now lead the table of new-to-market buyers.
- Lack of understanding of exposure and coverage options remain the primary obstacles to selling cyber insurance.
- The cyber insurance market appears to be increasing in consistency and price, even amid stronger competition. This represents a change from last year's survey. However, the remaining lack of consistency in terms of policies and language is prompting brokers to stick to the carriers that they know and trust.
- We also asked respondents to weigh in on hot-button issues, such as whether funds transfer fraud coverage should be available under crime or cyber policies (insurers said crime, brokers agreed but were more flexible.)
- GDPR issues continue to concern the market and its impact remains unclear. Many respondents expect only limited impact until there are headline losses.

Key Survey Findings 2018

'Third-party requirements' are a top-3 driver of cyber sales – **42%** of respondents



Seeking **dedicated limits** is a top-3 reason for switching **endorsement to standalone** -**70%** of respondents



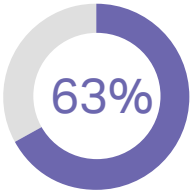
New-to-market buyers

- **90%** are SMBs
- Manufacturing sector now in **2nd place**

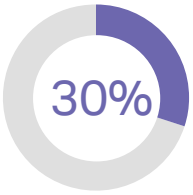
2018 market more competitive than **2017 - 90% of respondents**

33% named 'Regulatory change' as a top-3 sales driver

Which coverage are buyers most interested in?
BI beats data breach to top spot!

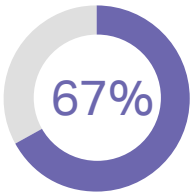


63% of insurers actively manage risk aggregation in-house

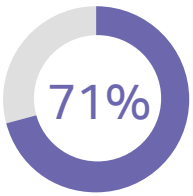


Pricing is very disjointed - **30%** of brokers

Underwriters felt more strongly than brokers that **cyber-related PD** belongs under a **property policy**



67% of brokers limiting number of carriers used to improve consistency



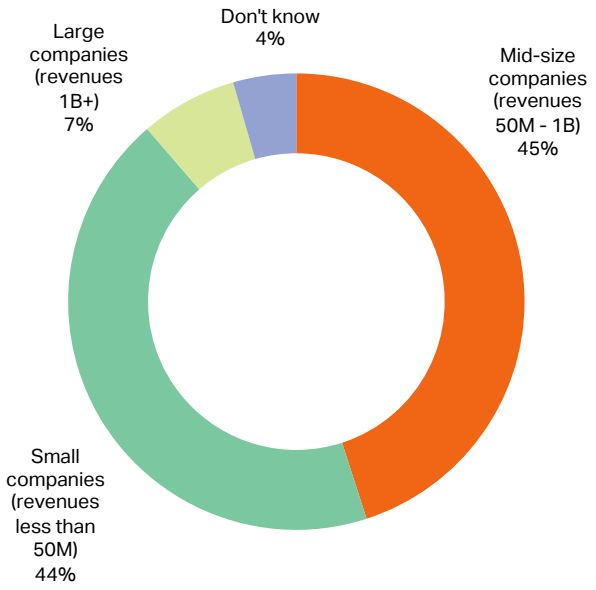
GDPR won't have much impact without a headline loss – **71%** of respondents

Shifting Sales

Most new buyers are SMBs

The survey revealed an influx of new-to-market buyers of standalone cyber insurance, the majority of them smaller (categorized as businesses with revenues of less than $50 million) and mid-sized businesses (revenues of $50 million to $1 billion). This may reflect an already higher insurance take-up rate among larger organizations, but the trend remains heartening, an indication that smaller businesses are beginning to more fully understand their risks.

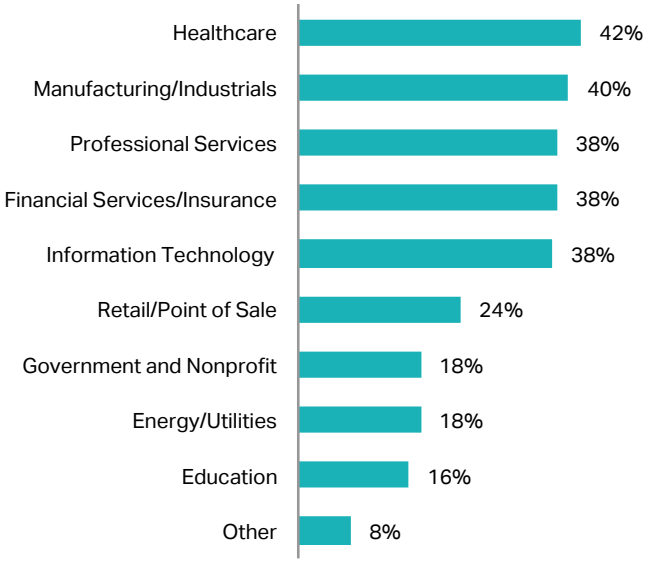
Q The majority of our new-to-market buyers of standalone cyber insurance are (including those switching from endorsements):



Healthcare and manufacturing now top the new buyer list

Across all sizes of business, underwriter respondents reported seeing new buyers (as well as new standalone coverage buyers) largely from the healthcare and manufacturing sectors.

Q What industries bring the most new to market buyers of cyber insurance? (select top 3)



For broker respondents, healthcare buyers took the top spot, although manufacturing, financial services/ insurance and professional services were not far behind.

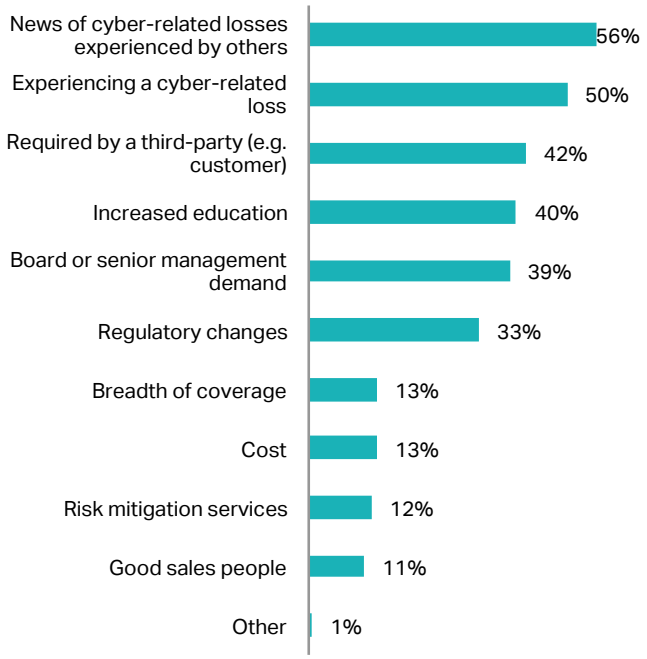
Overall, the manufacturing sector came in second, up from fifth place last year. While no respondents specifically commented on the 2017 NotPetya cyberattack, given that headline losses are the primary motive of sales (see following section), it seems likely that that's what's driving the manufacturing sector to buy.

Several brokers also commented on an increase in demand from the construction sector, as well as from hotel operators, which may be a response to the highly publicized breaches in the hospitality industry.

News of cyber events still top driver of cyber sales

The primary reason for buying cyber coverage, as in previous years, was in response to news of cyber events. The second-most common reason was the experience of a cyber-related loss. As one commenter wrote, "Some don't consider until after an occurrence. Then they buy quickly."

Q What do you see as the top driver(s) of cyber product sales? (select up to 3)



Another respondent noted "small companies are starting to feel the need to protect themselves with cyber insurance but it is still very hard to sell at this time unless they are closely related to a breach or required to put a policy in place."

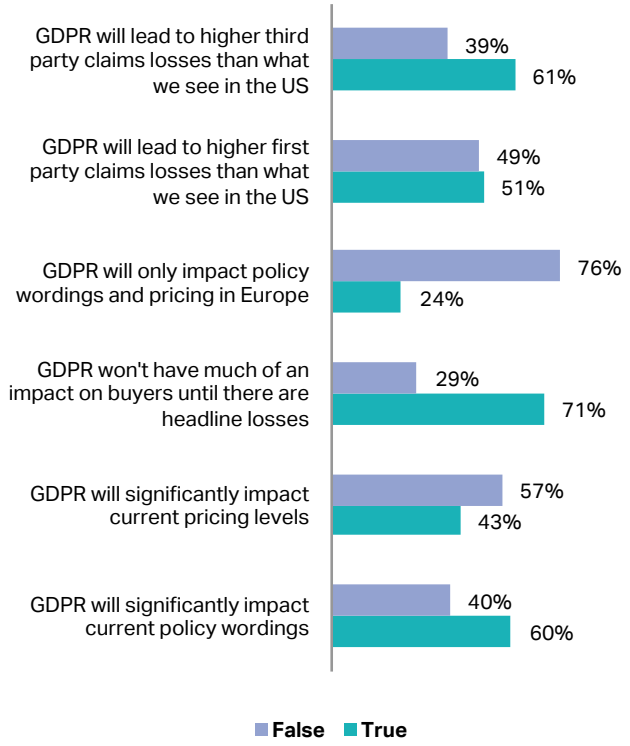
> "The primary reason for buying cyber coverage, as in previous years, was in response to news of cyber events."

And indeed, the third-most common reason behind a purchase is that coverage is 'required by a third party'. This suggests that attention continues to be paid to cyber risk throughout supply chains and in vendor relationships – and that this is driving more buyers to the market.

In another question relating to market growth, we asked about requests for higher limits at renewal: 60% of brokers and underwriters agreed that their clients are 'sometimes' interested in higher limits at renewal, 20% of respondents noted frequent interest in higher limits.

Regulation is driving sales, but GDPR impact remains unclear

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



33% of respondents selected 'regulatory changes' as a top-three driver of cyber product sales (see previous section). With the implementation of the European Union's General Data Protection Regulation (GDPR)

on May 25, 2018, regulatory requirements have both driven more buyers to the cyber market and posed the question of whether there will be an impact on coverage, pricing, and claims due to enforcement actions.

> "Until a breach or violation of GDPR results in a major fine, it seems doubtful that the regulation will have much impact on cyber policies." Survey respondent, 2018

66% of respondents felt that GDPR will have an impact on policy wordings in the market, while 43% said that it will affect pricing. However, 71% also said that there's unlikely to be any dramatic change until we start seeing headlines about losses and enforcement actions. Many brokers stated that organizations still don't understand the implications of GDPR and that the potential effects are "nebulous."

"Until a breach or violation of GDPR results in a major fine, it seems doubtful that the regulation will have much impact on cyber policies. That said, if there is a fine related to a violation that does not neatly fit within the wording of typical cyber policies, it does seem likely that there will be a push to expand cyber coverage to encompass that kind of violation of GDPR," said one respondent.

Another offered a view of the change that they would like to see, commenting, "GDPR means that all insurers in this space have an obligation to offer privacy coverage that goes beyond disclosure injury. Brokers who don't point out whether collection practices are covered or not may face E&O claims, insurers selling forms without offering the cover may face bad faith situations."

The concern appears to be over the uncertainty, particularly on a financial front. One broker said, "For U.S. clients [with] Euro Zone exposure, it will be interesting to see this evolve. There is genuine 'fear' of overzealous regulatory money grab with fines."

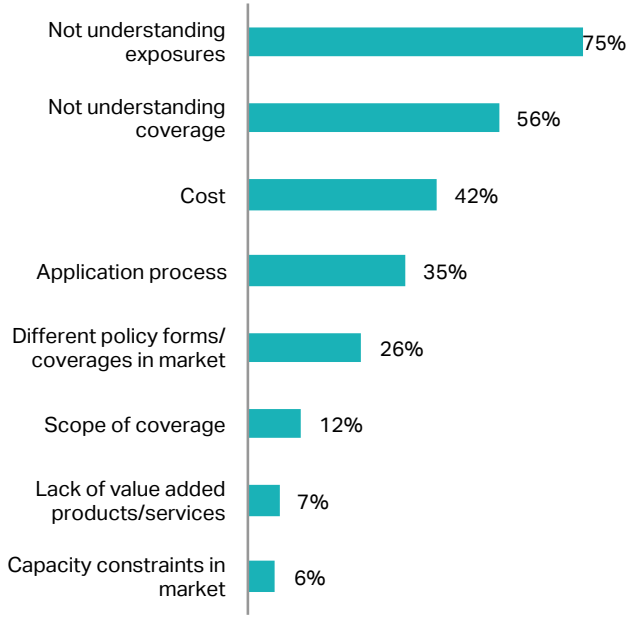
However, one respondent had a different view: "The focus with the GDPR is around fines. While significant, the insurability of these is looking more and more unlikely (though very much still a grey area). What has been overshadowed, is the likely heightened scope for collective third-party litigation afforded for under articles 80 & 82 of the GDPR."

Given the wide-range of comments on this topic, it's clear that there's no clarity yet as to GDPR's impact on the cyber insurance market going forward.

Lack of exposure understanding still the main obstacle to selling cyber

Regardless of the progress made in selling cyber coverage, challenges remain, say respondents. For both underwriters and brokers, the primary obstacle to sales continues to be a lack of understanding about the exposure; 75% of respondents felt that organizations simply don't understand their exposure. The second-highest response (56%) was clients 'not understanding coverage', a problem that may improve as consistency in coverage develops.

Q What are the biggest obstacles to writing cyber insurance policies? (select up to 3)



In some cases, respondents felt that the issue was one of overconfidence and belief by insureds that they don't have the type of data that cybercriminals would be interested in stealing. Many organizations forget, the survey revealed, that cyber risk increasingly involves more than just data breach, and is not just a problem for larger companies.

Clients often still assume "that they are not a target for breach because they are small or unknown compared to Target or Yahoo," said one broker. Another commented, "Despite going into great detail about the needs and coverages afforded, most clients think they are immune to the hackers."

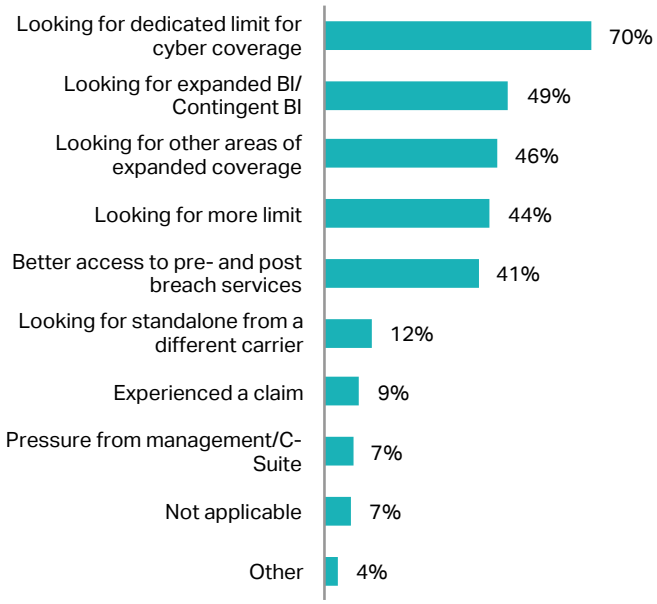
Several respondents reported that not all salespeople feel comfortable discussing the products since these are new to them and they've yet to build the expertise to confidently discuss the risk.

Coverage

Standalone covers more attractive than endorsements

In last year's survey, underwriters and brokers reported a shift from cyber endorsement to standalone policies, a shift that has continued over the past year, highlighting the value of a dedicated cyber insurance market.

Q If you have seen cyber business switch from endorsements to standalone policies, what is the main reason(s)? (select top 3)



We invited respondents to select their top three reasons for the shift. The most popular reason by far (70%) was buyers seeking the dedicated limits available expressly from cyber markets. Brokers and underwriters also reported clients seeking higher limits than they could acquire by endorsement (44%).

The second-most common reason for buyers turning to the standalone market was 'looking for expanded Business Interruption (BI)/contingent BI', which was also cited as the most popular coverage sought at renewal by cyber customers (see following section).

One broker offered some insight into the buying decisions, commenting in the survey, "As a broker we generally recommend against 'endorsement' cyber coverage. The coverage granted is very limited and creates somewhat of an illusion that the insured is covered for cyber threats, when in fact most of these endorsement coverages are narrow in scope and often with small limits."

Other reasons that generated a significant response for switching to standalone policies were that insureds were looking for other areas of expanded coverage, and for better access to pre- and post-breach services.

Only 9% of respondents attributed the switch to claims – suggesting that organizations see the sense in proactive buying behavior in looking for pure cyber coverage and/or are taking the advice of brokers who recommend the broader coverage and more specialized expertise in the cyber market. In one broker's view, "coverage in the endorsements falls well short of what is available in the standalone market and tends to come with inexperienced vendors services."

A few respondents commented that contractual obligations drove insureds to switch from endorsement to standalone policies, which is in line with the growth of third-party requirements as a driver of sales in the cyber insurance market.

Q If you write cyber endorsements, what line(s)?

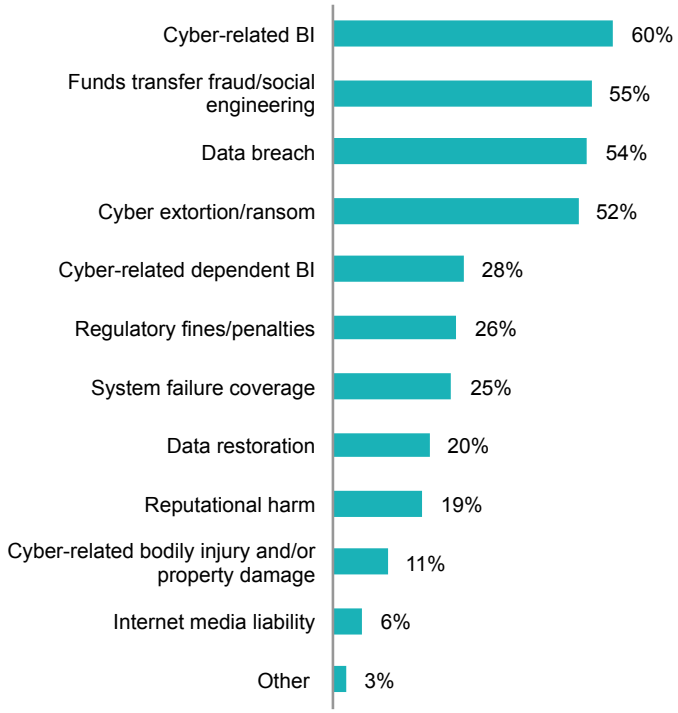
In instances where respondents write cyber endorsements on other lines of coverage, errors and omissions (E&O) coverage was the most commonly endorsed line at 72%, followed by directors and officers liability (D&O) and employment practices liability (EPL). Crime policies also saw a strong percentage of cyber endorsements, likely due to a rise in fraudulent instruction scams and funds transfer fraud. A few brokers also noted seeing cyber endorsements on marine and pollution policies, suggesting potential growth areas for the cyber insurance product.

> "Where respondents write cyber endorsements on other lines of coverage, errors and omissions (E&O) coverage was the most commonly endorsed line."

Cyber-related BI now the most-requested coverage

As similarly noted in the previous section on reasons for switching to standalone, new and renewal cyber buyers most frequently requested cyber-related BI coverage (62% of underwriters and 59% of brokers). For the first time since we began this survey, cyber-related BI has now replaced data breach as the most sought-after coverage.

Q What cyber coverages are new and renewal buyers most interested in purchasing? (select top 3)



Data breach remained a close second for 56% of underwriter respondents, but fell to third place for brokers after funds transfer fraud coverage. 40% of underwriters selected funds transfer fraud coverage as a top-three request, placing it in fourth place.

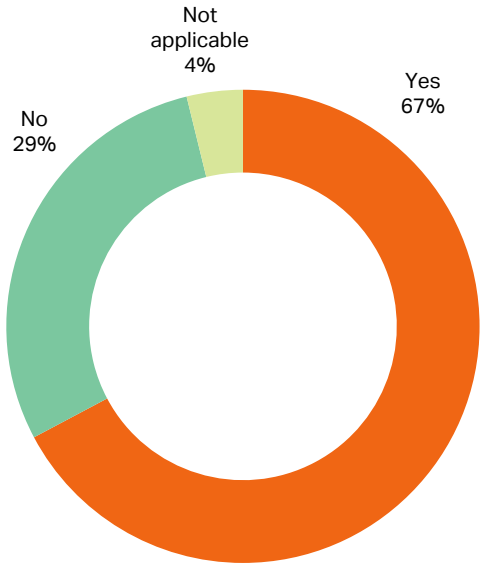
For brokers, buyers seeking cyber extortion/ransom coverage tied with data breach for third place. Broker comments to this section indicated that their view tends to be: when in doubt, cover everything. The type of business being insured also factors into the most commonly requested coverages, brokers reported.

"Our position is to present 'full featured' coverage and often not presenting coverage as a pick-and choose menu but rather 'all in'," said one broker.

Consistency increasing, as is competition

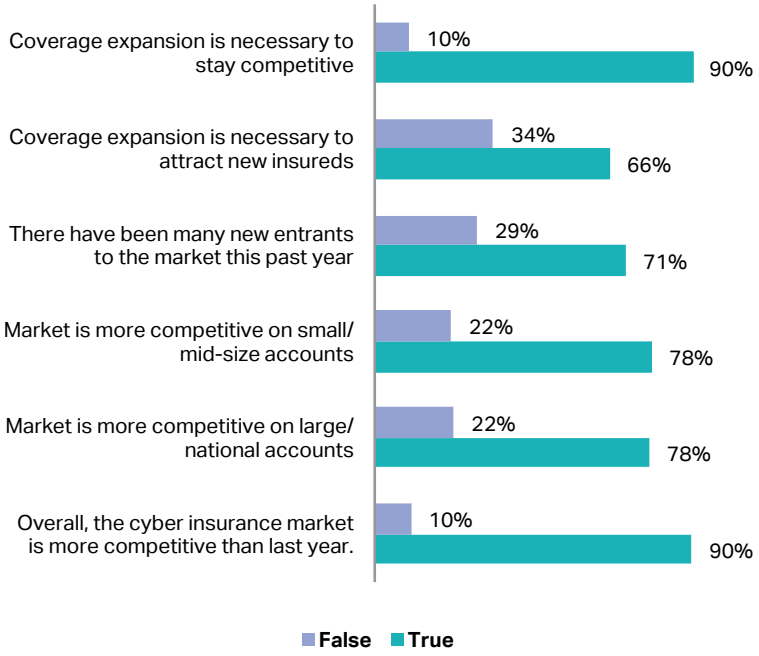
We asked brokers to weigh in on pricing and coverage consistency. The verdict – both are becoming more consistent, but there's still considerable variation and it's perhaps not surprising then that 67% of brokers continue to limit the number of carriers that they work with to limit their exposure to different policies and wordings. Broker commentary focused largely on "verbiage is not consistent," "there is still enough difference that you really have to look at the terms you are being offered," but that there is more consistency "over broader coverages."

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



Regarding competition, broker and underwriter respondents almost unanimously agreed that the market is more competitive than last year – 90% answered 'true' to this question. Overall, respondents felt that the market is now as competitive in the SMB space as it is for larger organizations. However, if we just look at underwriter respondents, they felt that the SMB space was more competitive than the large/national accounts sector. And 71% of respondents agreed that there are more insurers offering cyber insurance coverage this year than in 2017. That may not be a good thing according to some respondents, who also felt that only the specialists are likely to rise to the top.

Q Please answer true or false to the following:



One commenter said, "I believe that the market will winnow out carriers who do not truly have a cogent cyber insurance strategy that seeks to serve its customers with a view toward the long term -- and I think customers will benefit from that, as only 'serious' carriers will remain in the space. I just don't know when that is going to happen."

> "67% of brokers continue to limit the number of carriers that they work with to limit their exposure to different policies and wordings. "

Overall, the market continues to improve in consistency, 57% of broker respondents said that they see more consistency in coverage, versus 34% seeing no increase. Broker comments provided a fuller picture of the trends behind these percentages, with a clear message of frustration coming from the broker world, many of whom feeling that more reliably consistent results from insurers and policies would aid in increasing cyber insurance take-up rates.

One respondent noted, "There are clusters of carriers who have consistent pricing, with a couple of underwriters on the extremes (high and low). But these are not the same carriers from customer to customer, so there isn't a great sense of cohesiveness or predictability in pricing."

The most prominent players in the market are driving consistency, according to survey responses. One broker said, "Revised forms from established carriers in the space are being released now, so policy language is also fairly competitive as carriers work to match the language of the leaders in the market."

Others agreed, noting, "Carriers are still all over the place, even internally. There are maybe 15 underwriters who are consistent." Another said, "Across the board, no, coverage is not consistent. However, there are 5-10 carriers that offer standalone policies with consistent coverages."

One broker expressed a common view by saying, "The breadth of cyber coverage is fine. In fact it's too much. What is needed to improve the cyber line is support services pre- and post- breach and risk management and security services. Loss prevention is key because even with insurance, a cyber loss poses difficult recovery."

However, most brokers (70%) answered 'true' to the question of whether coverage expansion is necessary to attract new insureds. Underwriter respondents were almost evenly split (48% to 52%) on this question. Many respondents (90%) agreed that coverage expansion is also necessary to remain competitive – we interpret this result to signify that carriers that do not provide coverage that is at least in line with what is offered by most will be at a competitive disadvantage.

One underwriter comment reflected another view of the market with "I personally think coverage is already expansive enough, we are getting plenty of new interest, any more additions to coverage and we are going to be covering nearly anything even remotely associated with cyber or the internet. Plus, coverage is already overlapping significantly with D&O/EPLI, crime, property, medical malpractice, etc. Any more will cause even more significant overlap."

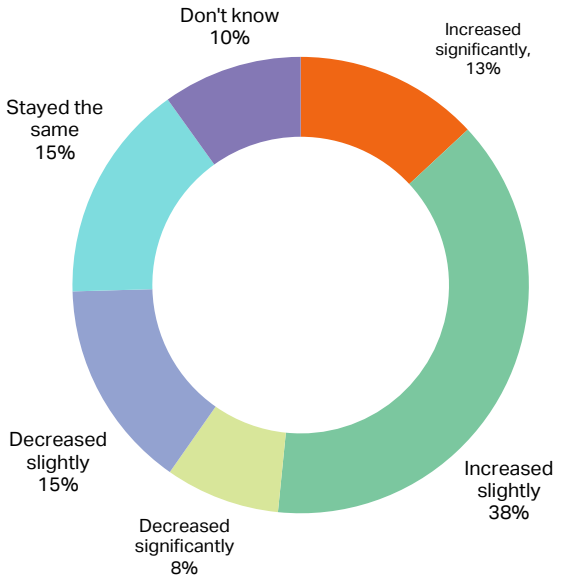
Differences of opinion around policies and perils

Several questions on our survey aimed to clarify cyber gaps, overlaps and responding policy issues.

Coverage overlaps

Overlaps in coverage appear to have become more evident over the last year – 38% of respondents said they feel that overlaps have 'increased slightly' and 13% feel that they have 'increased significantly'.

Q Coverage overlap between cyber and other policies has:



As the market expands, different views have emerged as regards which policies are the right place for cyber-related BI and property damage, as well as for social engineering/funds transfer fraud.

Cyber vs property/GL

Based on the responses, there in any case appears to be only occasional interest from insureds for cyber-related BI and property damage coverage – and it is not universally available in the market, with less than half of underwriter respondents saying that they offer the coverages as part of their cyber policies or endorsements. 41% of underwriters said that insureds 'sometimes' show 'real interest' in buying it. 37% said insureds 'rarely' show interest.

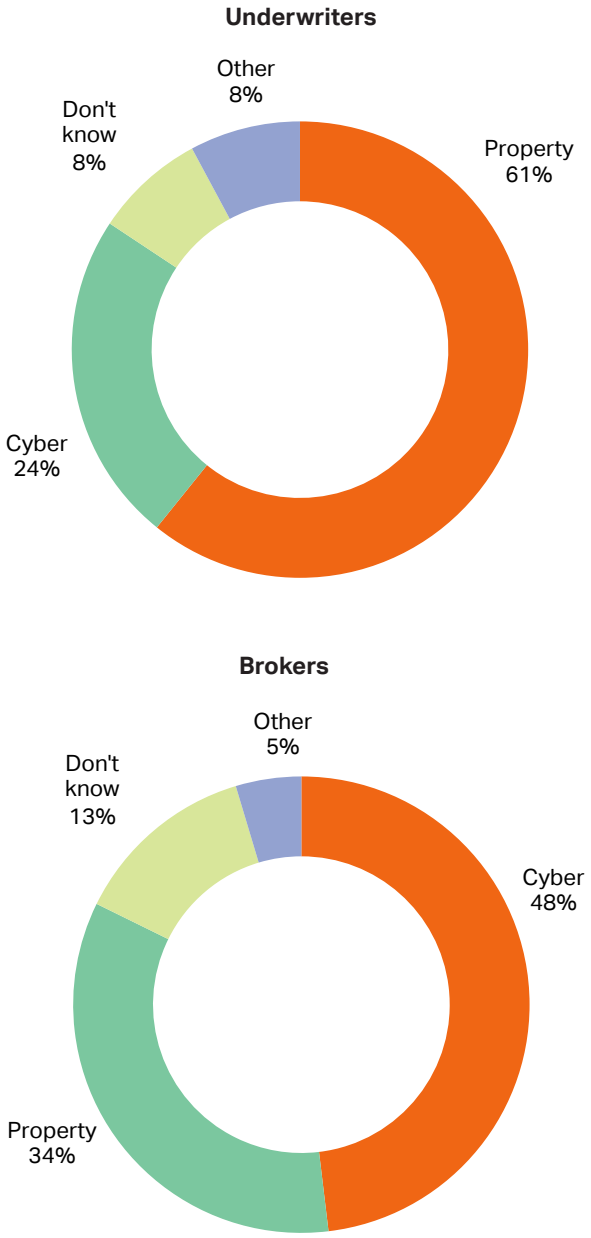
Conversely for brokers, the firm belief that their clients may need this cover drives them to press for it, even though 43% agreed that their clients 'rarely' show interest in having the coverage on their cyber policies. 'Frequent' interest is rare, reported by just 10% of broker respondents, while 32% said that their clients show interest 'sometimes'.

"They don't see the big risk here. Usually it's enough to restore the programs and data inside," said one broker. Another added, "That doesn't mean we don't try and get it or get it if we believe [they need it]." Most noted that interest and need depends on the industry, usually falling to utilities and manufacturing clients.

"This coverage is not well known or understood, and pricing can be prohibitive and/or not available depending on the class," said one broker.

The real divide between underwriters and brokers came when we asked whether cyber-related property damage should be covered under a property or cyber policy.

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



The majority (60%) of underwriters felt that the property policy should handle the risk. Nearly half (48%) of brokers said a cyber policy would be better suited. However, brokers showed a lot of flexibility on this point in their comments.

"It depends," said one broker. "The property market is more prepared from a capacity standpoint for the type of loss itself, but the scenario will not be a classic BI/PD trigger if it is a cyber incident. The policyholder needs the expertise of a cyber-forward market and all the other buckets of coverage that could trigger - including forensics, BI, and management of the event itself - as well as the payout for the property loss."

> "Now that cyber policies are becoming more common, other lines of coverage are reducing their scope of coverage. Clients do not want to have their GL limits eroded by a cyber loss." Survey respondent, 2018

Another stated, "I think it depends on the industry. But if there is real catastrophic exposure, I think the property market may be better suited to underwrite. Some cyber insurers consult with their property counterparts to underwrite the BI/PD exposure and that is probably the best approach."

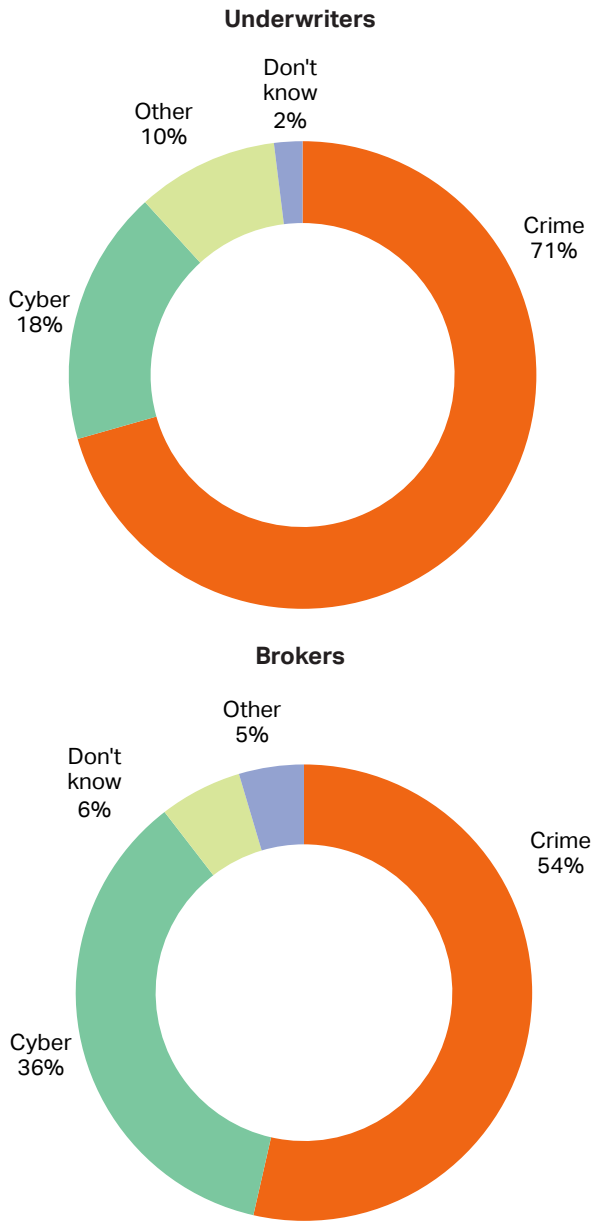
Other broker suggestions included basing the policy that first responds on the type of incident, or expecting cyber policies to cover financial loss and property policies to handle tangible property damage. A clear message from brokers came through: cyber underwriters, talk to your property counterparts.

"Now that cyber policies are becoming more common, other lines of coverage are reducing their scope of coverage. Clients do not want to have their GL limits eroded by a cyber loss," said one broker. Others said they see problems due to "vague language" in property policies and some see cyber claims being paid under kidnap/ransom, crime computer fraud, and property policies, which further blurs the lines.

Cyber vs crime

The issue of cyber versus crime policies for funds transfer fraud/social engineering has been a hotspot for discussion and legal activity in the past year. Although 66% of insurers offer this cover frequently or on occasion in cyber policies, just over 70% of these respondents thought that it should in fact be covered under crime policies.

Q Do you believe funds transfer fraud loss due to social engineering is better covered by a cyber policy or a crime policy?



On the other hand, a few commenters appeared open to letting the market decide or to going on a case-by-case basis, with one noting, "I'm of two minds on this. But the industry has seemed to accept it as a cyber issue due to market concerns" and another stating, "Doesn't matter. Customer should buy it on whatever policy they want to."

For the most part, brokers agree on both points. Just over half (53%) said that they feel a crime policy should

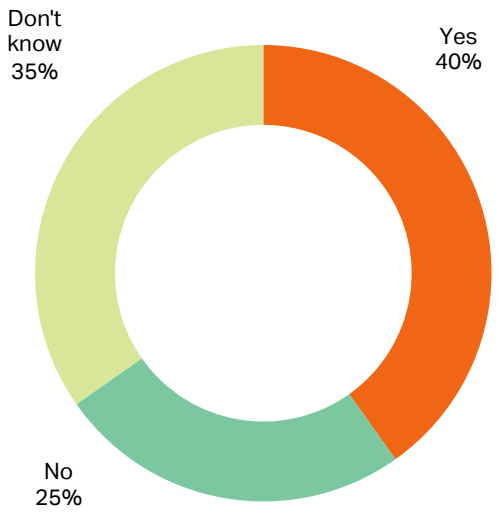
respond, while 35% said cyber. Others see a blended response, with one broker saying, "Both: the crime should pick up the financial loss and the cyber should respond to deal with first-party costs for what clearly was a cyber intrusion."

Claims

Claims experience matters

As cyber claims increase, so do examples of insurers differentiating themselves by claims handling – 40% of brokers said that they've noticed a difference in claims handling. One broker said, "Claims handling is the primary reason we place coverage with the carriers we do."

Q Have you noticed a difference in claims handling among carriers?



Common themes among brokers' comments on claims handling include a desire for speedy service – while this might seem obvious to insurers, brokers offered more advice, noting a need for not only fast but easy access to breach services.

And more experience is better, with cyber insurance specialists the preferred option – one broker explained, "Proven, established carriers have experienced claims staff versus an unproven carrier using a third-party claims service."

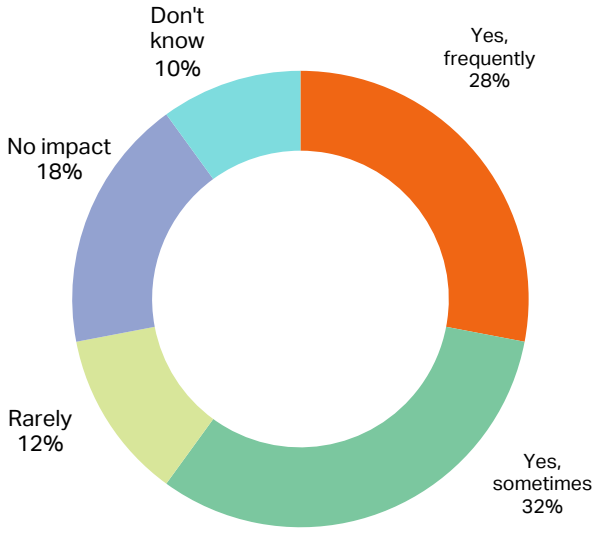
Many brokers commented that their clients have not had to file a claim. In fact, almost 35% of brokers were unable to answer the questions about claims handling.

Risk Aggregation

Most insurers are managing risk aggregation in-house

Given that risk aggregation is such a hot topic in the cyber market, we asked underwriters to comment on their aggregation management and found that most (62%) manage their risk aggregation entirely in-house, without the assistance of outside vendors. Just under 16% said that they use an outside firm to help manage risk aggregation, while nearly 10% said that they don't know their firm's approach to aggregation. Nearly 8% said, 'No, but we're working on it' when asked if they actively manage aggregation.

Q Is aggregation management impacting your underwriting or pricing decisions?



Aggregation does appear to be having an impact on pricing and underwriting decisions, with underwriter respondents saying that there is an impact either 'frequently' (28%) or 'sometimes' (32%).

Overall Satisfaction

Cyber market still only 'sometimes' meeting customer needs

A common answer to many of the questions asked in this year's survey was 'Yes, but it depends' or 'Yes, sometimes'. That theme followed through when we asked brokers whether they felt that the cyber insurance market meets the needs of its customers – with 77% answering 'sometimes', the answer essentially boils down to: yes, but there's room for improvement!

Brokers highlighted areas where they feel that insurers could improve, along with acknowledging the limitations as regards their clients' budgets and lack of awareness of risk that can affect the comprehensiveness of coverage purchased.

"Carriers are trying to anticipate possible claims scenarios and response scenarios for insureds and trying to write policy forms to address these scenarios; insureds often underestimate their exposure and agents don't have enough experience to answer customer objections, assess exposures, and suggest adequate limits of coverage needed," one broker commented.

Another said, "I would say 'always,' but the 'needs of insureds' is an inherently subjective term. Carriers may view an insured's actual needs differently than the insured does (and the insured may choose not to buy certain elements of a cyber policy that a carrier believes would address insured needs)."

One broker summed it up by saying, "We always need to do a better job."

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 solutions.

How can we help?

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

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

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

Your contacts

Andrew Laing:
Cyber P&C North America
andrew.laing@partnerre.com
+1 203 485 8438

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

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

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.