

We are pleased to present key raw survey data from our 2018 Survey of Cyber Insurance Market Trends, with the aim of increasing transparency and widening the potential for extended use and analysis across the industry.

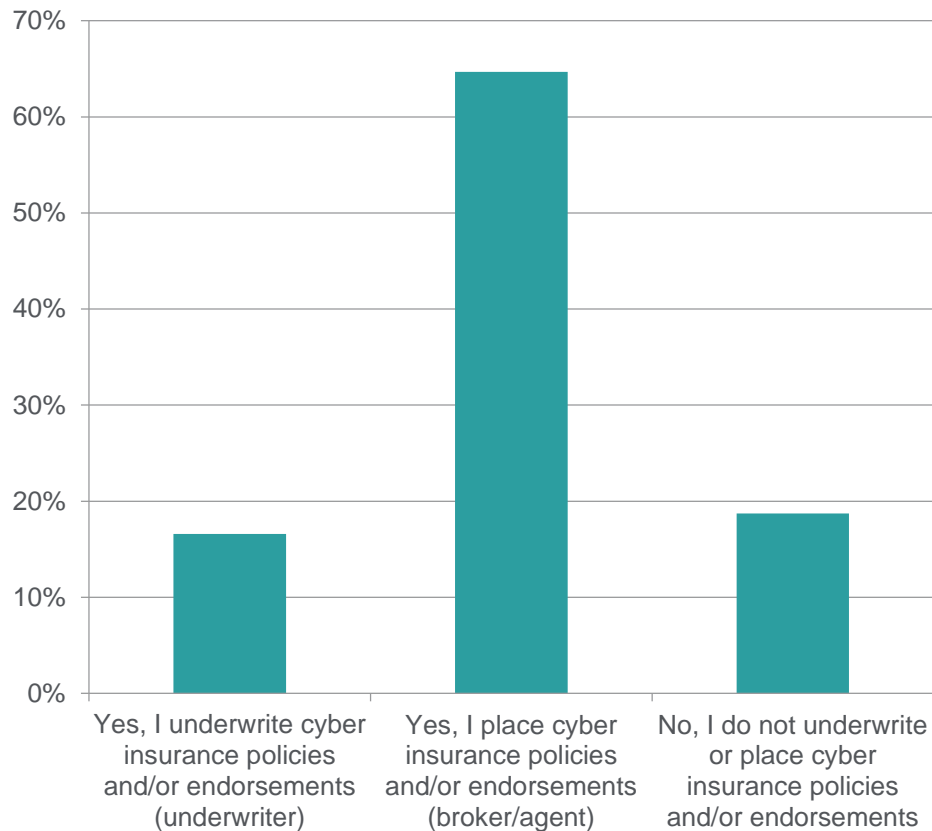
The main survey report - a summary and discussion of the survey findings - is available to download under www.partnerre.com/opinions-research

If you would like to reproduce or disseminate this data, please note: Information (excluding the survey respondent comments in slides 33 to 38 which are included only as a point of interest and may not be reproduced or disseminated in any way) contained in this document can only be reproduced or disseminated in the context of the evolving cyber insurance market and should be cited as follows: ‘Source: PartnerRe and Advisen, 2018 Survey of Cyber Insurance Market Trends’.

2018 Survey of Cyber Insurance Market Trends

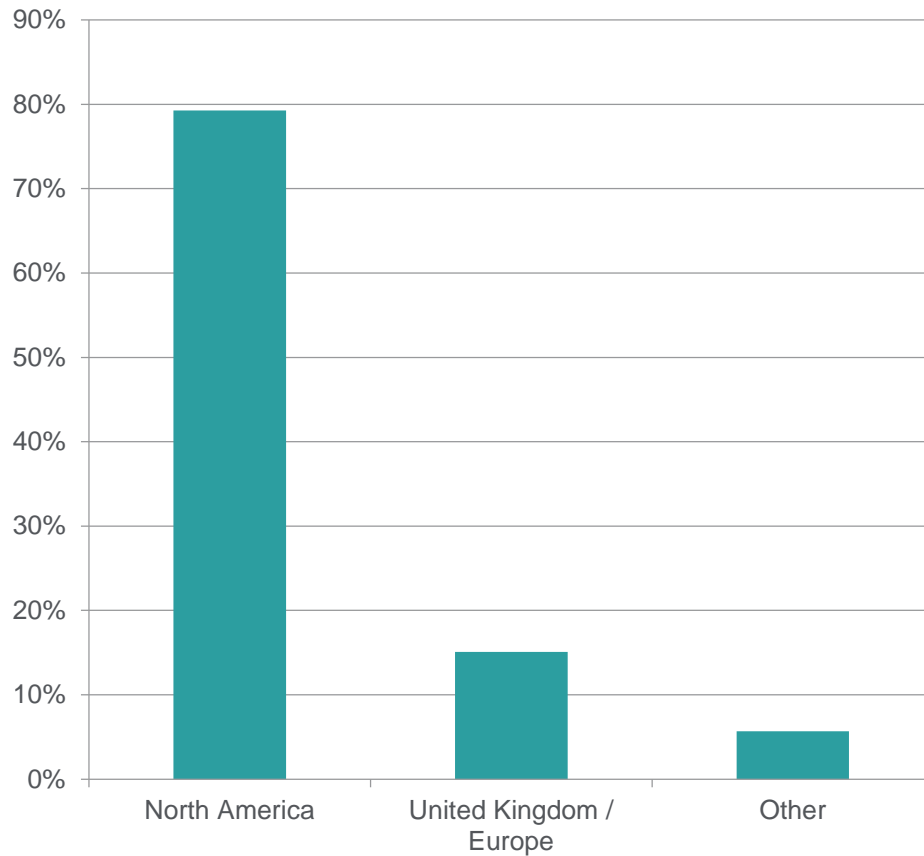
Supporting Raw Data

Do you underwrite or place cyber insurance policies and/or endorsements?



Answer Choices	Responses	
Yes, I underwrite cyber insurance policies and/or endorsements (underwriter)	17%	70
Yes, I place cyber insurance policies and/or endorsements (broker/agent)	65%	273
No, I do not underwrite or place cyber insurance policies and/or endorsements	19%	79
	Answered	422
	Skipped	0

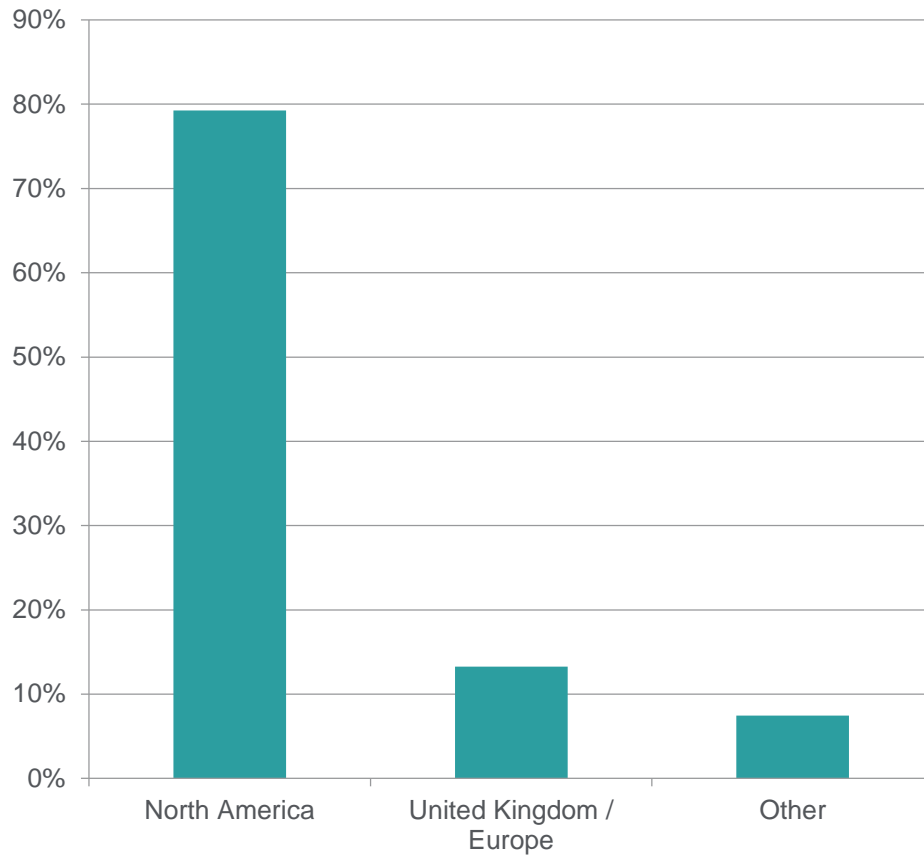
I am located in



Question to underwriters

Answer Choices	Responses	
North America	79%	42
United Kingdom / Europe	15%	8
Other	6%	3
	Answered	53
	Skipped	369

I am located in



Question to brokers

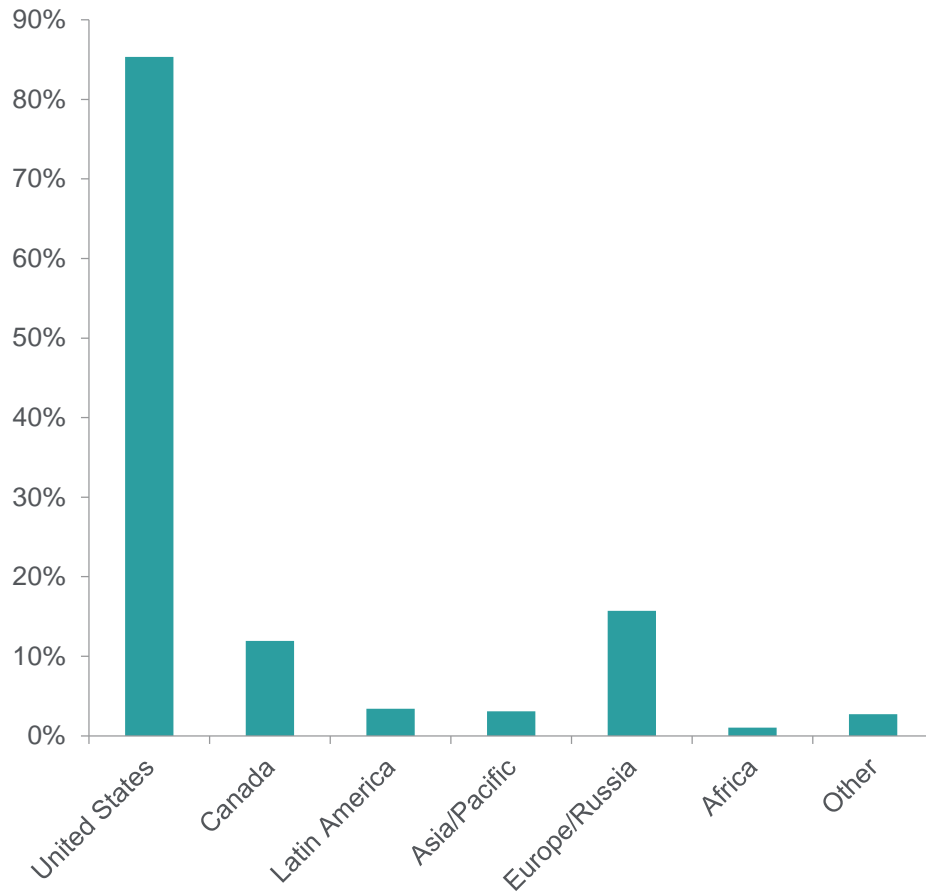
Answer Choices	Responses	
North America	79%	191
United Kingdom / Europe	13%	32
Other	7%	18
	Answered	241

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data



At least 10% of insureds I see are located in (check all that apply):

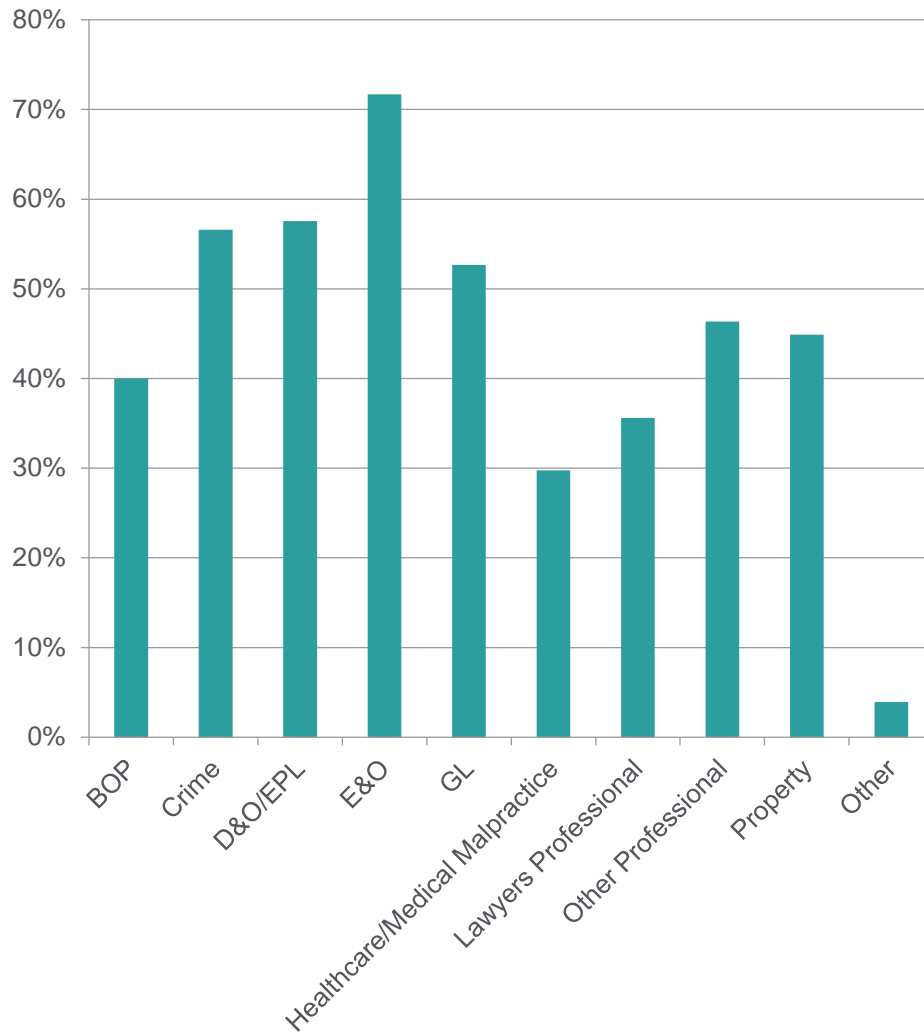


Answer Choices	Responses	
United States	85%	250
Canada	12%	35
Latin America	3%	10
Asia/Pacific	3%	9
Europe/Russia	16%	46
Africa	1%	3
Other	3%	8
Answered		293

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data

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

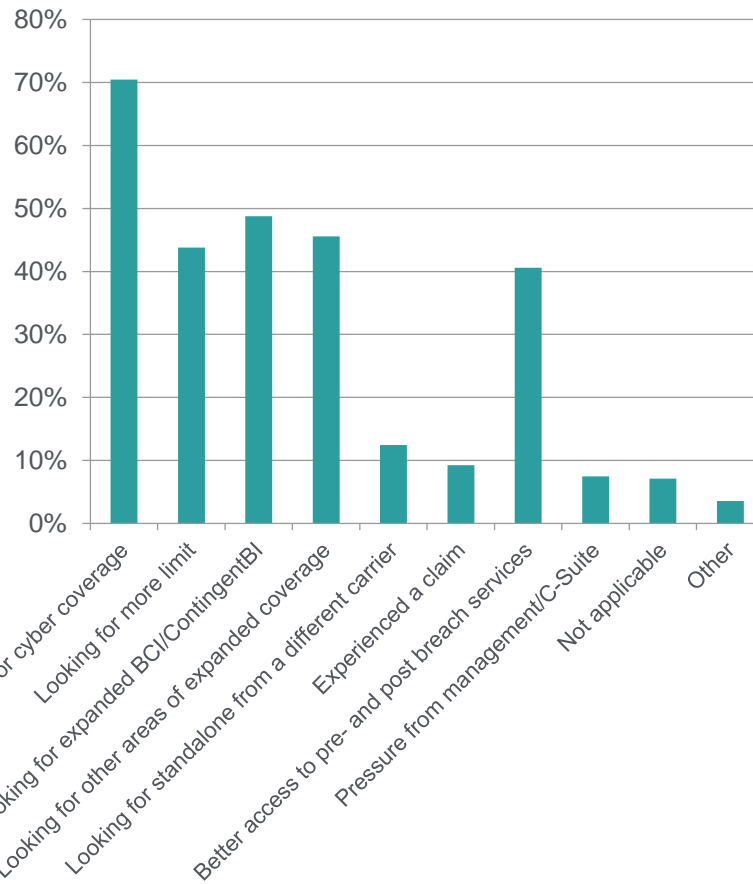


Answer Choices	Responses	
BOP	40%	83
Crime	57%	116
D&O/EPL	58%	118
E&O	72%	147
GL	53%	108
Healthcare/Medical Malpractice	30%	61
Lawyers Professional	36%	73
Other Professional	46%	95
Property	45%	92
Other	4%	8
Answered		205

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data

If you have seen cyber business switch from endorsements to standalone policies, what is the main reason(s) (pick maximum of top three):

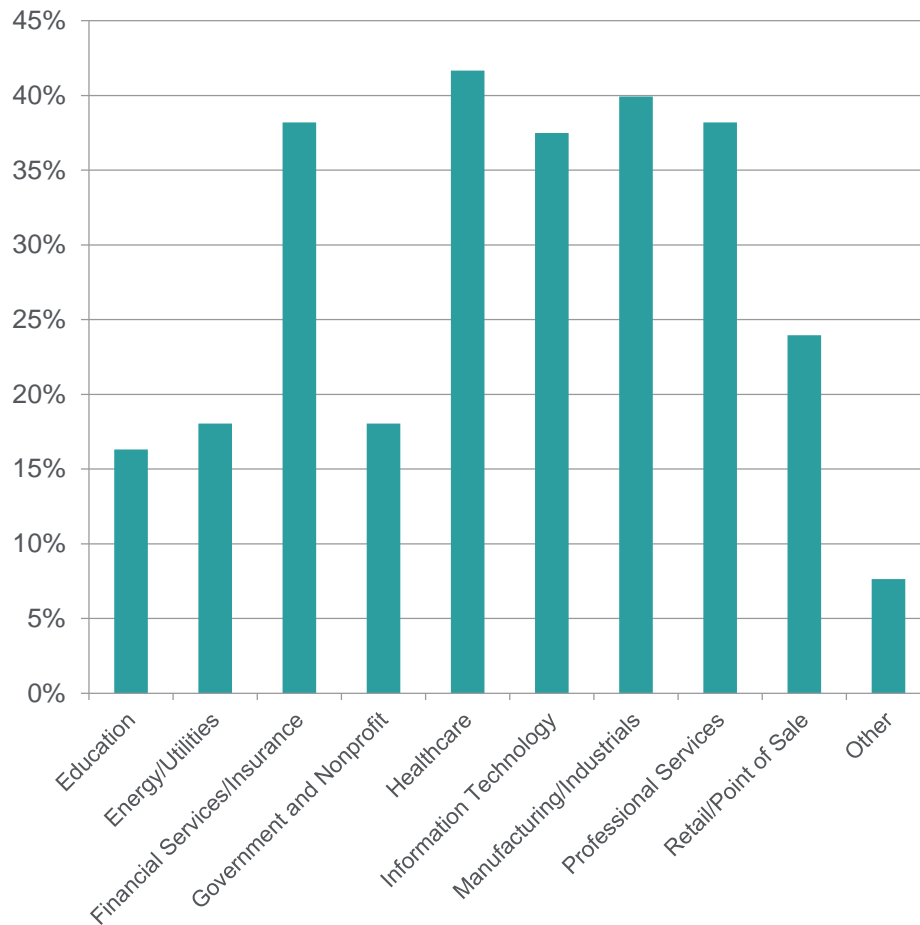


Answer Choices	Responses	
Looking for dedicated limit for cyber coverage	70%	198
Looking for more limit	44%	123
Looking for expanded BCI/ContingentBI	49%	137
Looking for other areas of expanded coverage	46%	128
Looking for standalone from a different carrier	12%	35
Experienced a claim	9%	26
Better access to pre- and post breach services	41%	114
Pressure from management/C-Suite	7%	21
Not applicable	7%	20
Other	4%	10
Answered		281

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data

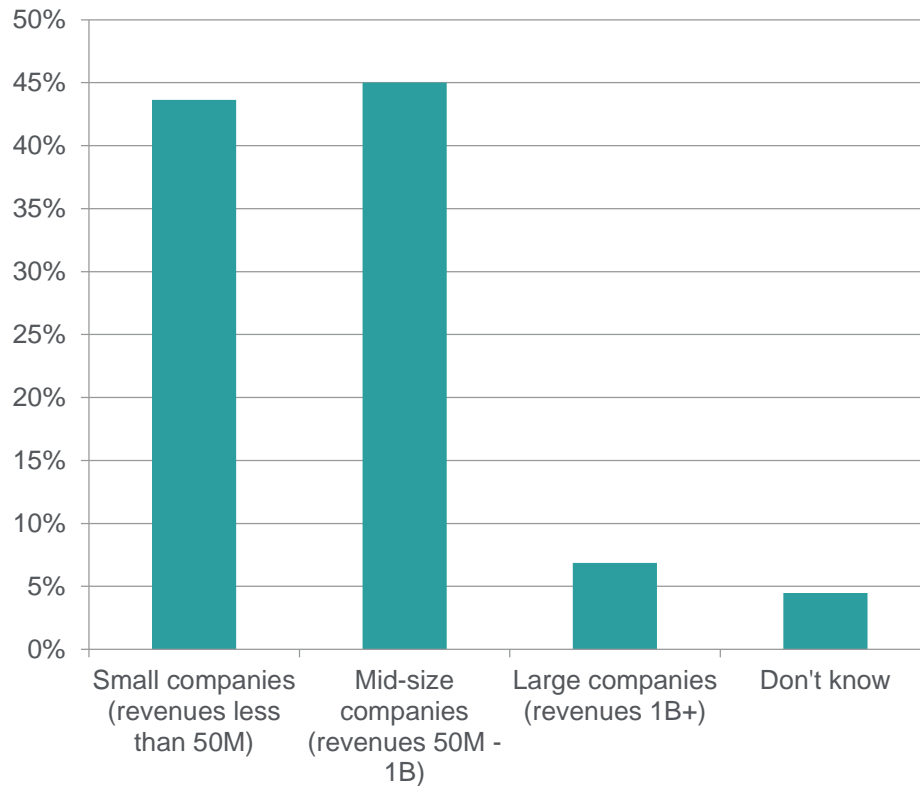
What industries bring the most NEW to market buyers of cyber insurance? (select top three)



Answer Choices	Responses	
Education	16%	47
Energy/Utilities	18%	52
Financial Services/Insurance	38%	110
Government and Nonprofit	18%	52
Healthcare	42%	120
Information Technology	38%	108
Manufacturing/Industrials	40%	115
Professional Services	38%	110
Retail/Point of Sale	24%	69
Other	8%	22
Answered		288



The majority of our NEW to market buyers of STANDALONE cyber insurance are (including those switching from endorsements):

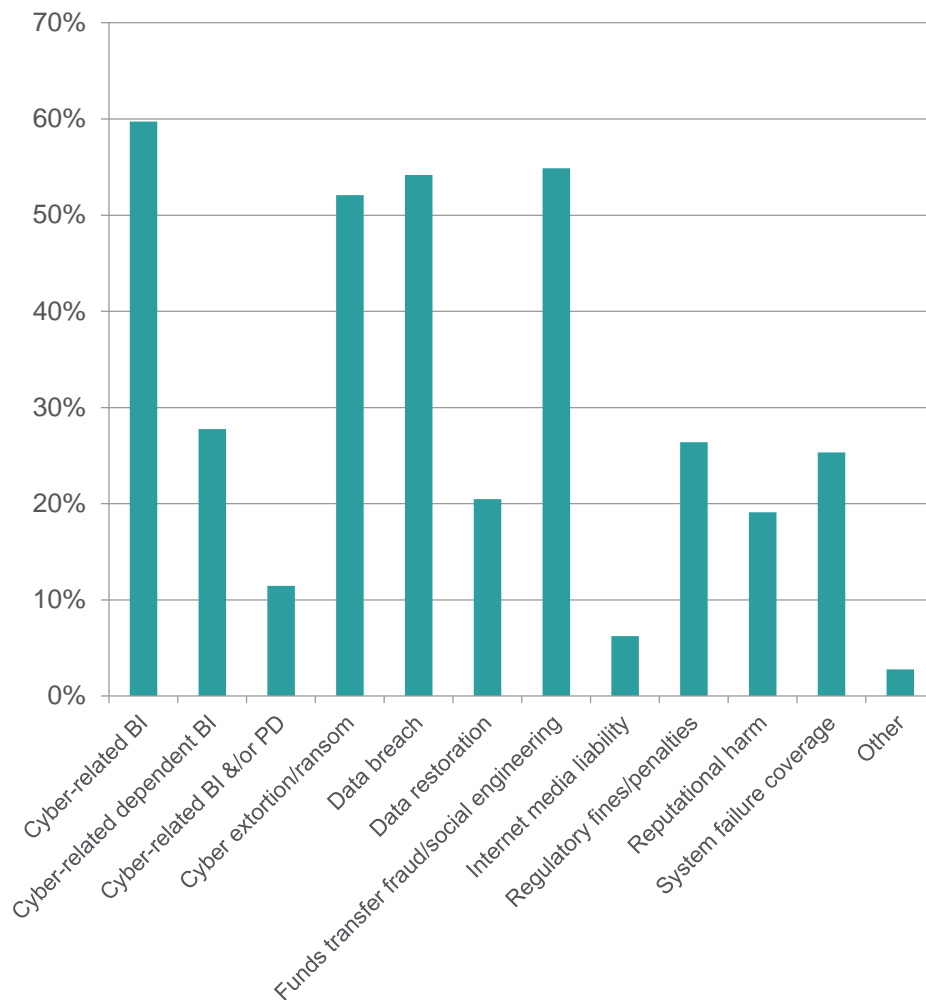


Answer Choices	Responses	Count
Small companies (revenues less than 50M)	44%	127
Mid-size companies (revenues 50M - 1B)	45%	131
Large companies (revenues 1B+)	7%	20
Don't know	4%	13
Answered		291

2018 Survey of Cyber Insurance Market Trends

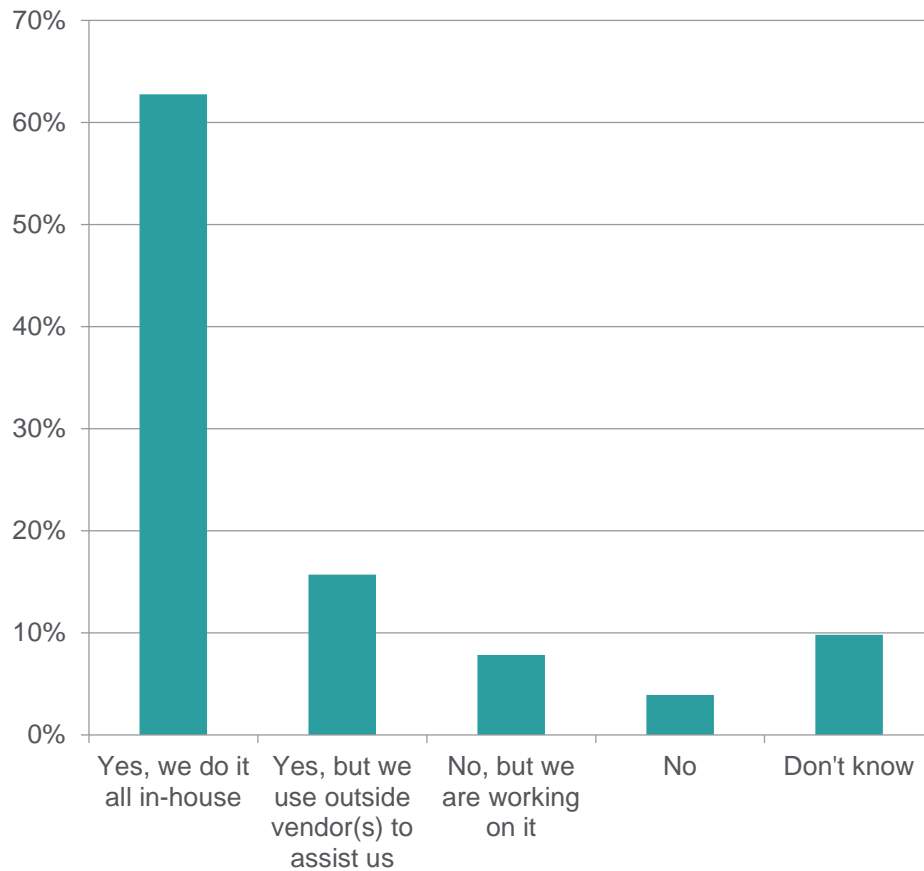
Supporting Raw Data

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



Answer Choices	Responses	
Cyber-related BI	60%	172
Cyber-related dependent BI	28%	80
Cyber-related BI &/or PD	11%	33
Cyber extortion/ransom	52%	150
Data breach	54%	156
Data restoration	20%	59
Funds transfer fraud/social engineering	55%	158
Internet media liability	6%	18
Regulatory fines/penalties	26%	76
Reputational harm	19%	55
System failure coverage	25%	73
Other	3%	8
Answered		288

Is aggregation actively managed by your company?

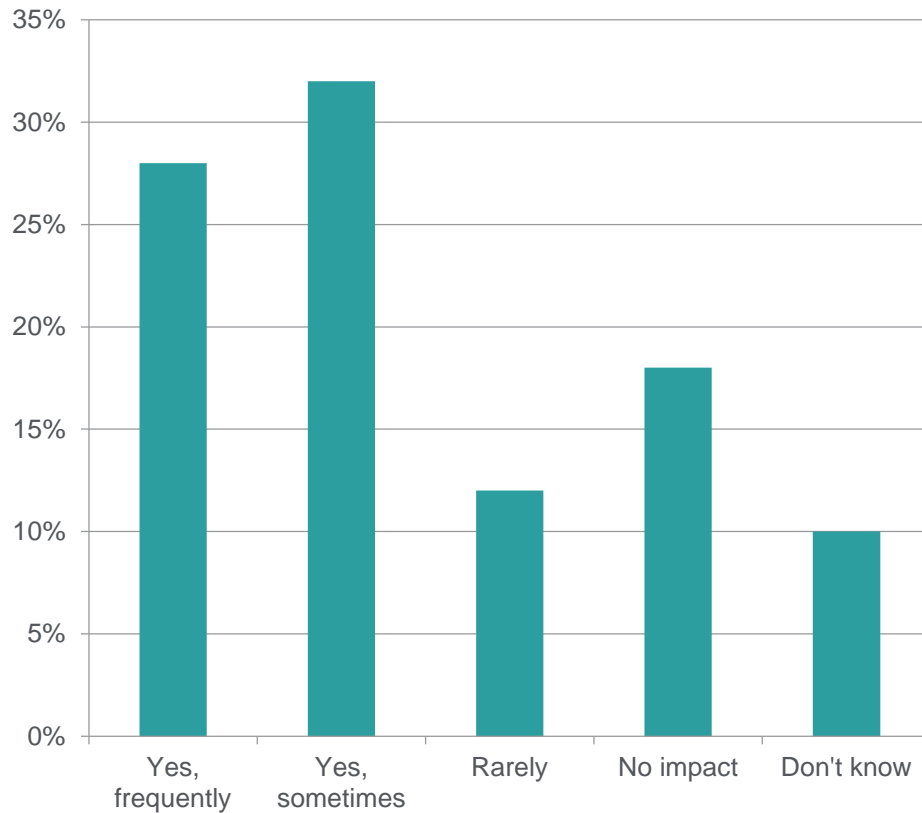


Question to underwriters

Answer Choices	Responses	Count
Yes, we do it all in-house	63%	32
Yes, but we use outside vendor(s) to assist us	16%	8
No, but we are working on it	8%	4
No	4%	2
Don't know	10%	5
No, we're not worried		1
Answered		51



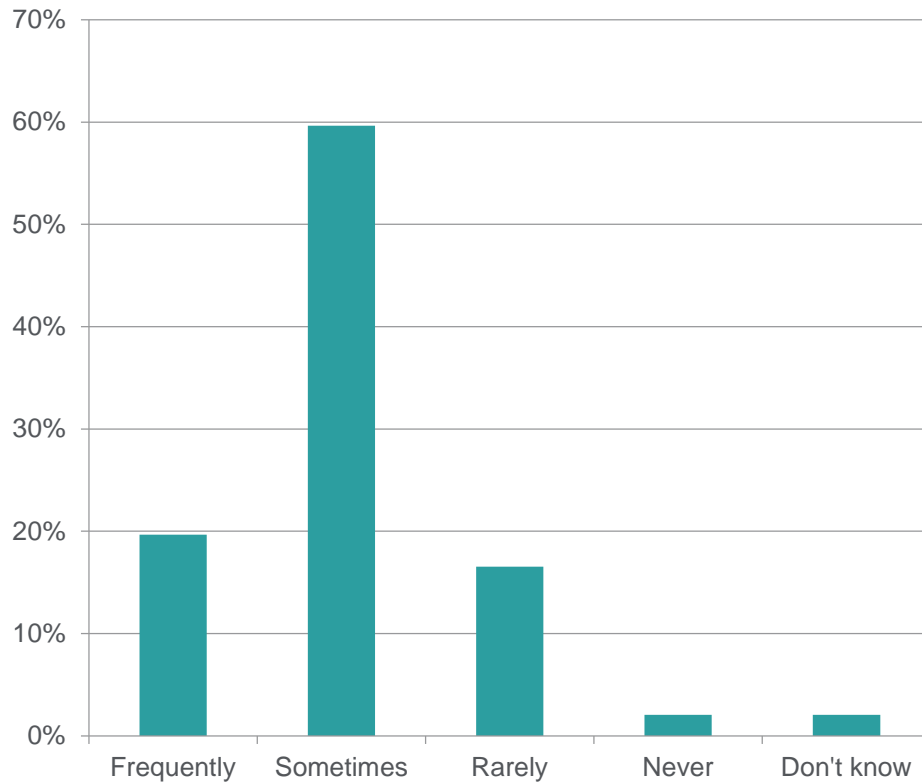
Is aggregation management impacting your underwriting or pricing decisions?



Question to underwriters

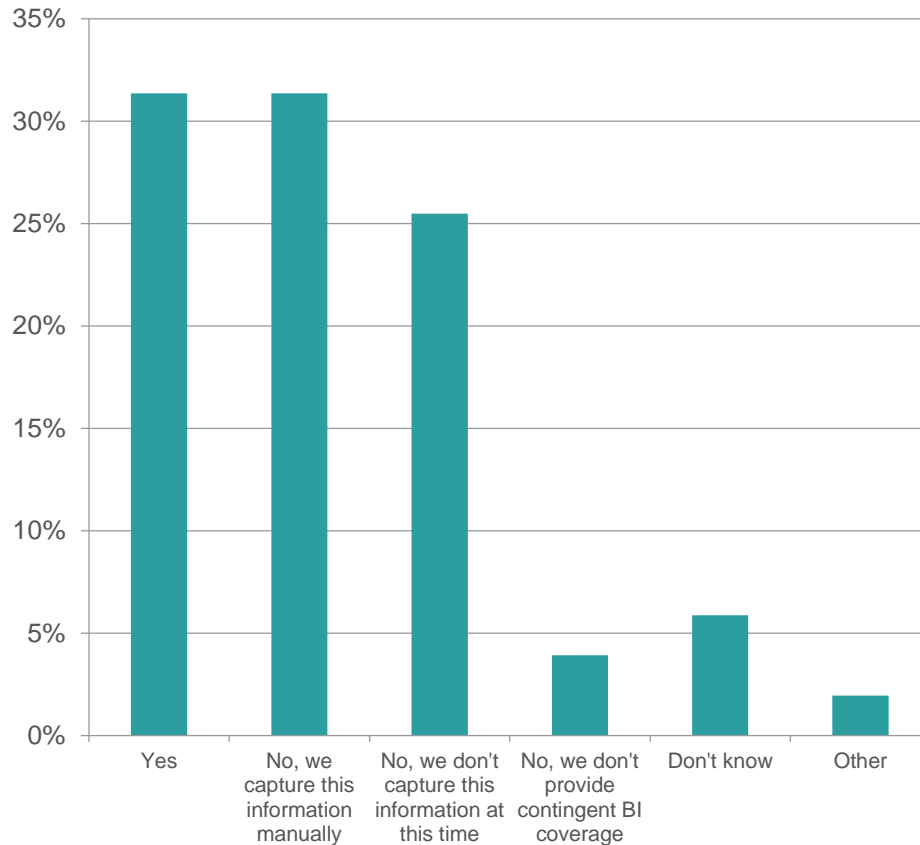
Answer Choices	Responses	
Yes, frequently	28%	14
Yes, sometimes	32%	16
Rarely	12%	6
No impact	18%	9
Don't know	10%	5
	Answered	50

Are your renewal insureds requesting higher cyber insurance limits?



Answer Choices	Responses	
Frequently	20%	57
Sometimes	60%	173
Rarely	17%	48
Never	2%	6
Don't know	2%	6
	Answered	290

Do you rely on vendor(s) to evaluate an insured's third-party relationships?

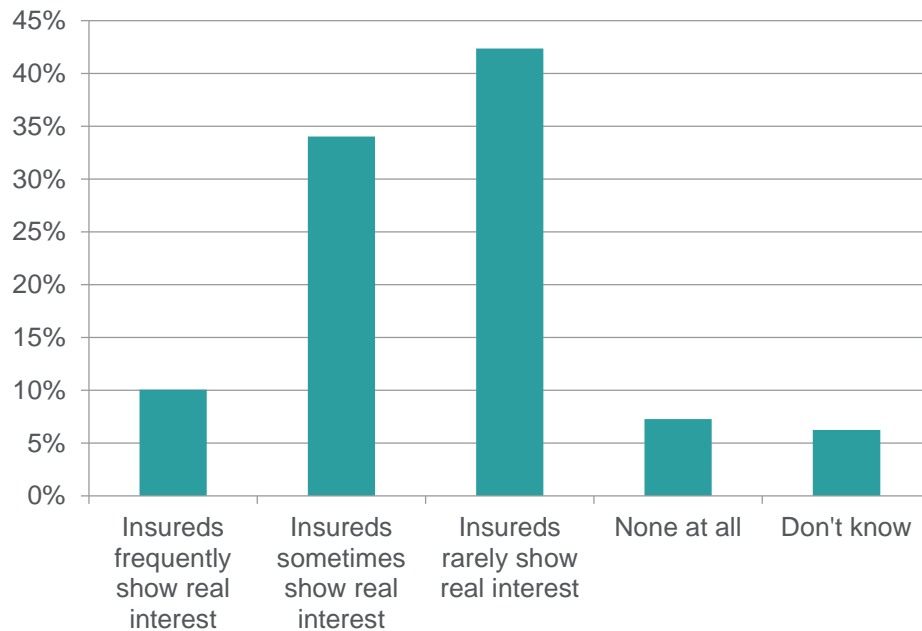


Question to underwriters

Answer Choices	Responses	Count
Yes	31%	16
No, we capture this information manually	31%	16
No, we don't capture this information at this time	25%	13
No, we don't provide contingent BI coverage	4%	2
Don't know	6%	3
Other	2%	1
Answered		51



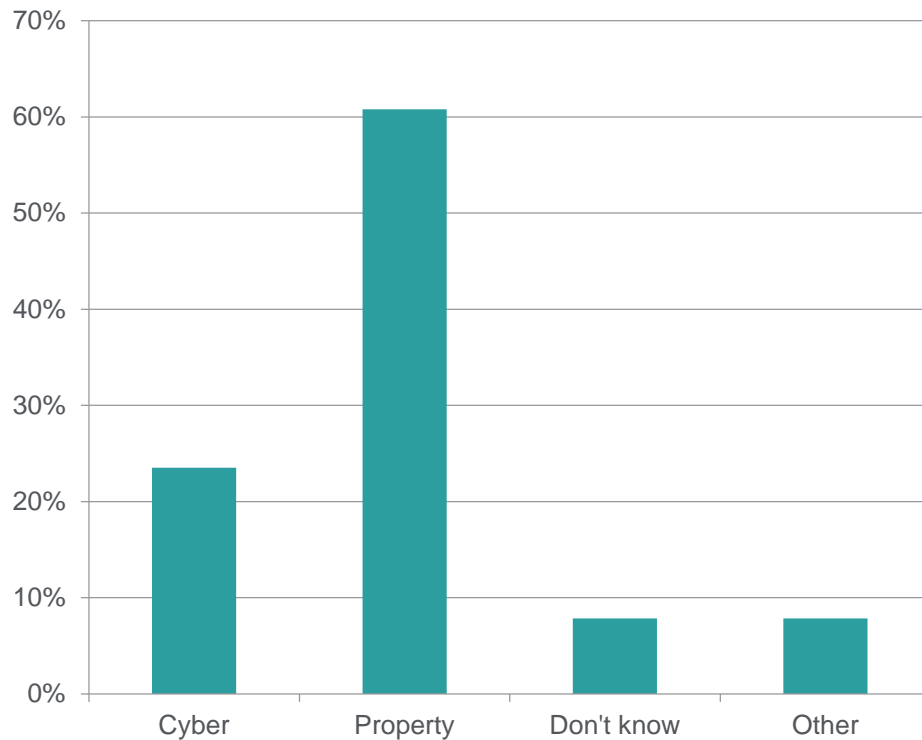
How much demand is there for cyber-related bodily injury and/or property damage coverage under the cyber policy?



Answer Choices	Responses	
Insureds frequently show real interest	10%	29
Insureds sometimes show real interest	34%	98
Insureds rarely show real interest	42%	122
None at all	7%	21
Don't know	6%	18
	Answered	288



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

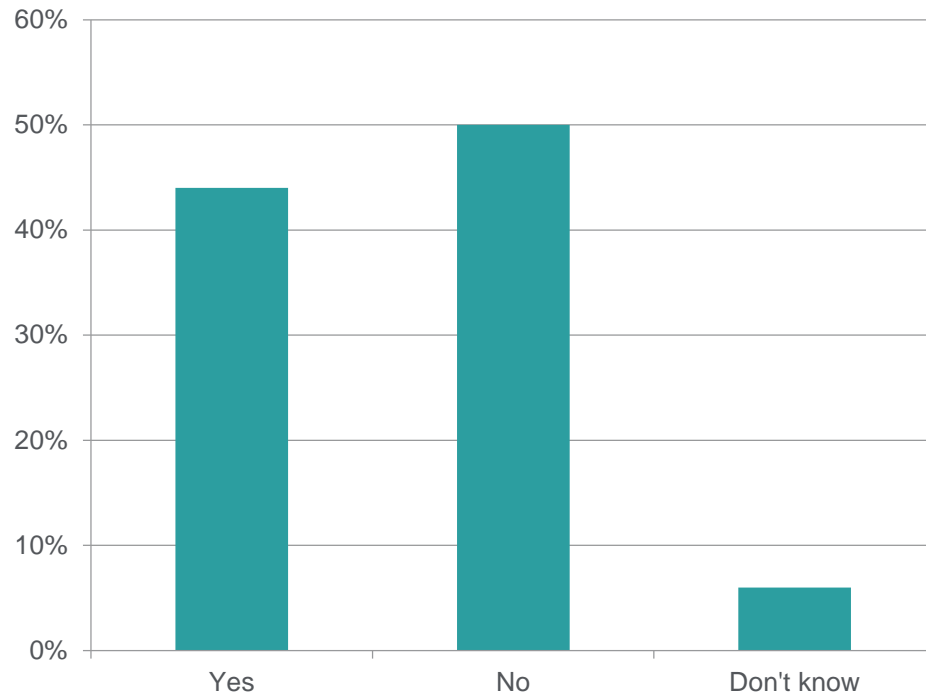


Question to underwriters

Answer Choices	Responses	
Cyber	24%	12
Property	61%	31
Don't know	8%	4
Other	8%	4
	Answered	51



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

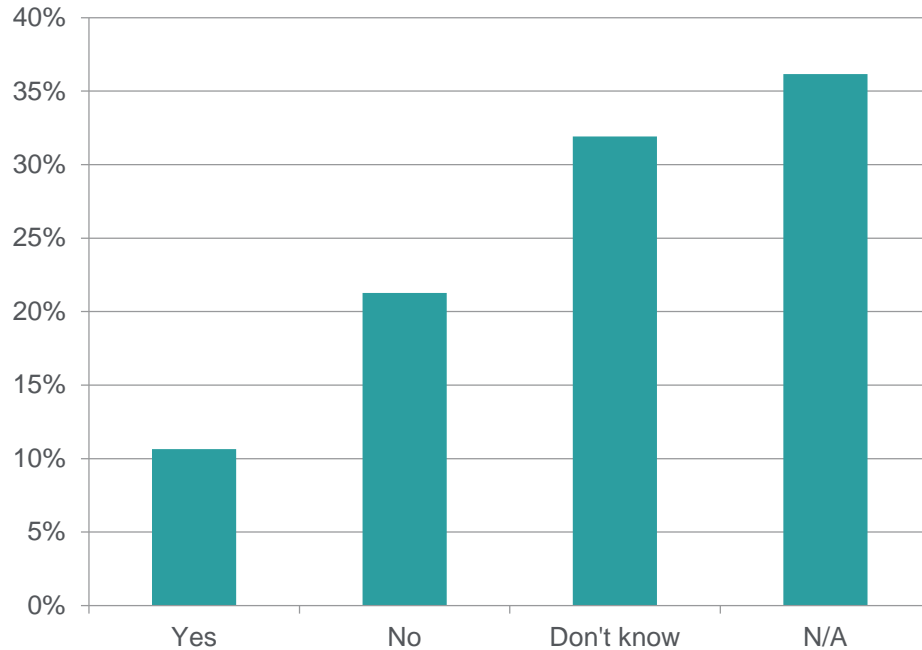


Question to underwriters

Answer Choices	Responses	
Yes	44%	22
No	50%	25
Don't know	6%	3
Answered		50



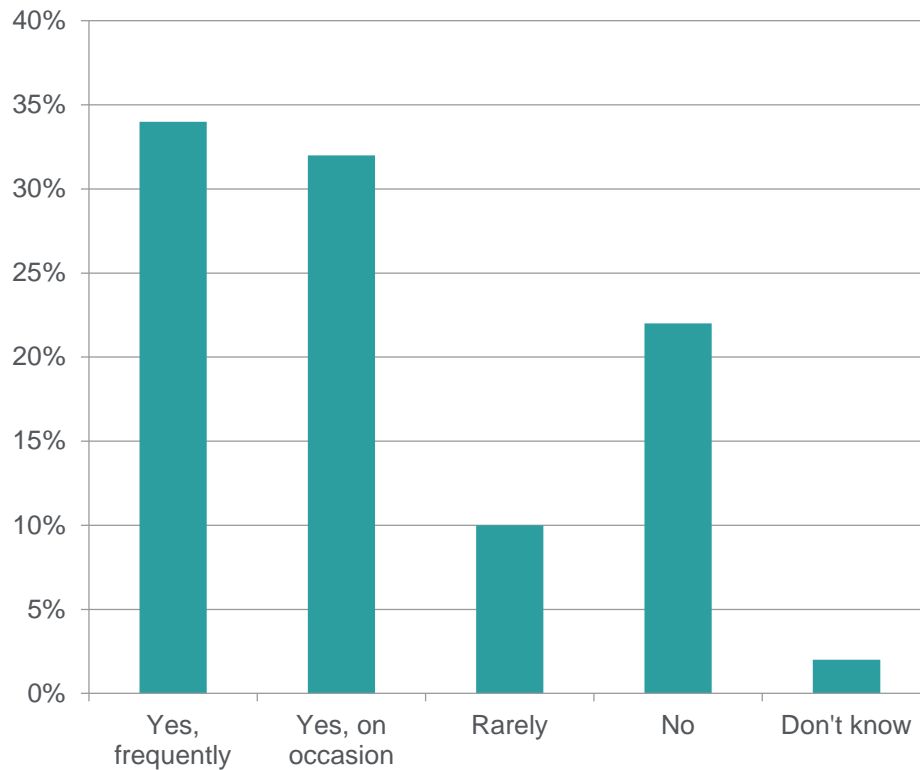
If your company's cyber insurance policy or endorsement does not currently provide coverage for cyber-related bodily injury and/or property damage, does it plan to in the future?



Question to underwriters

Answer Choices	Responses	
Yes	11%	5
No	21%	10
Don't know	32%	15
N/A	36%	17
	Answered	47

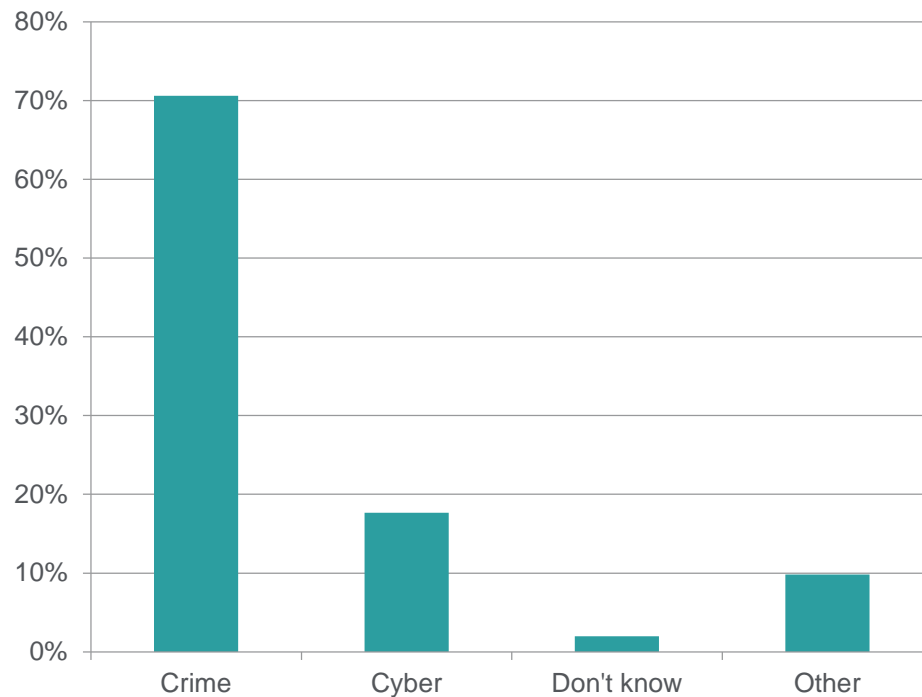
Does your company provide funds transfer fraud loss coverage with the cyber insurance policy?



Question to underwriters

Answer Choices	Responses	
Yes, frequently	34%	17
Yes, on occasion	32%	16
Rarely	10%	5
No	22%	11
Don't know	2%	1
Answered		50

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



Question to underwriters

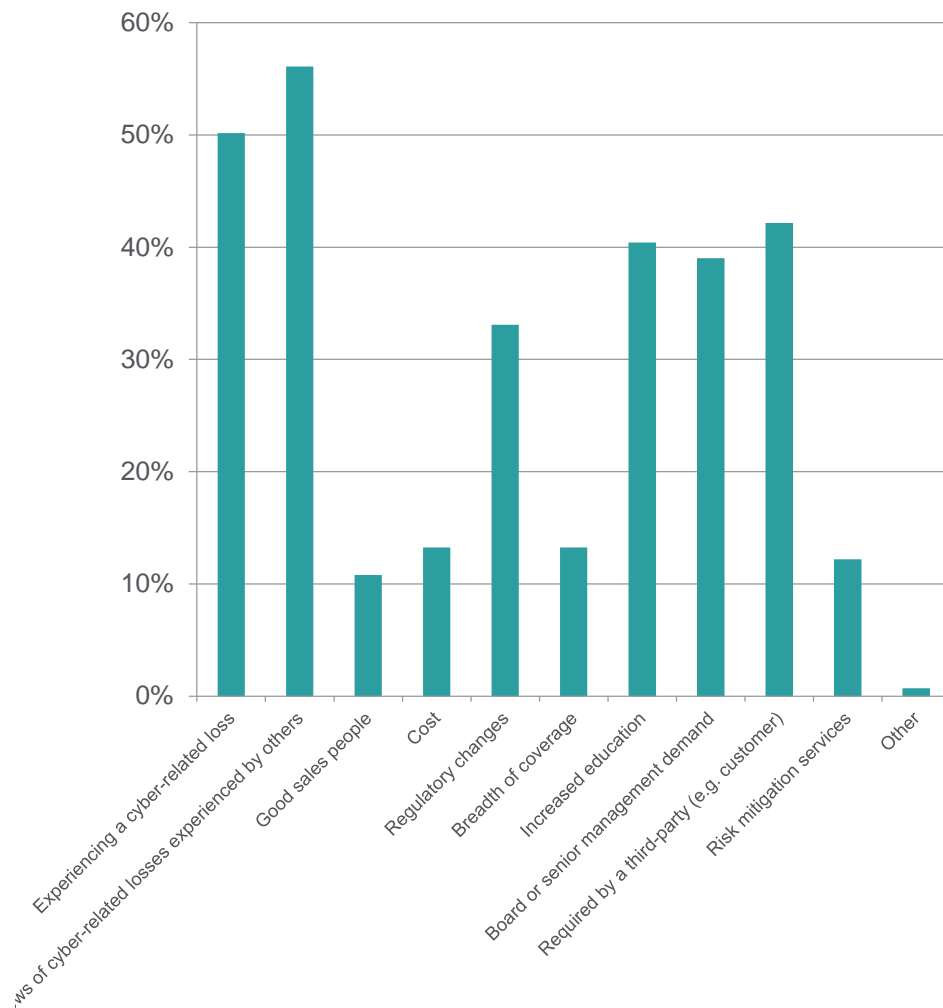
Answer Choices	Responses	
Crime	71%	36
Cyber	18%	9
Don't know	2%	1
Other	10%	5
	Answered	51

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data



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



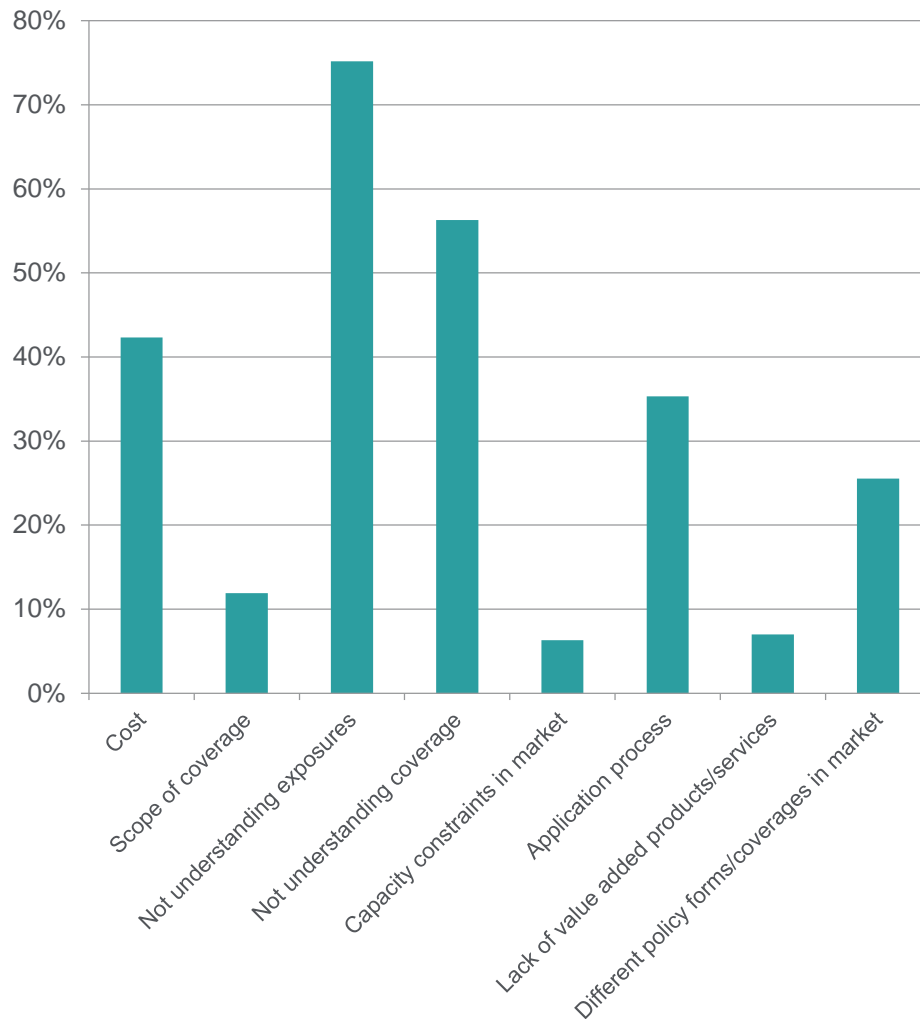
Answer Choices	Responses
Experiencing a cyber-related loss	50% 144
News of cyber-related losses experienced by others	56% 161
Good sales people	11% 31
Cost	13% 38
Regulatory changes	33% 95
Breadth of coverage	13% 38
Increased education	40% 116
Board or senior management demand	39% 112
Required by a third-party (e.g. customer)	42% 121
Risk mitigation services	12% 35
Other	1% 2
Answered 287	

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data

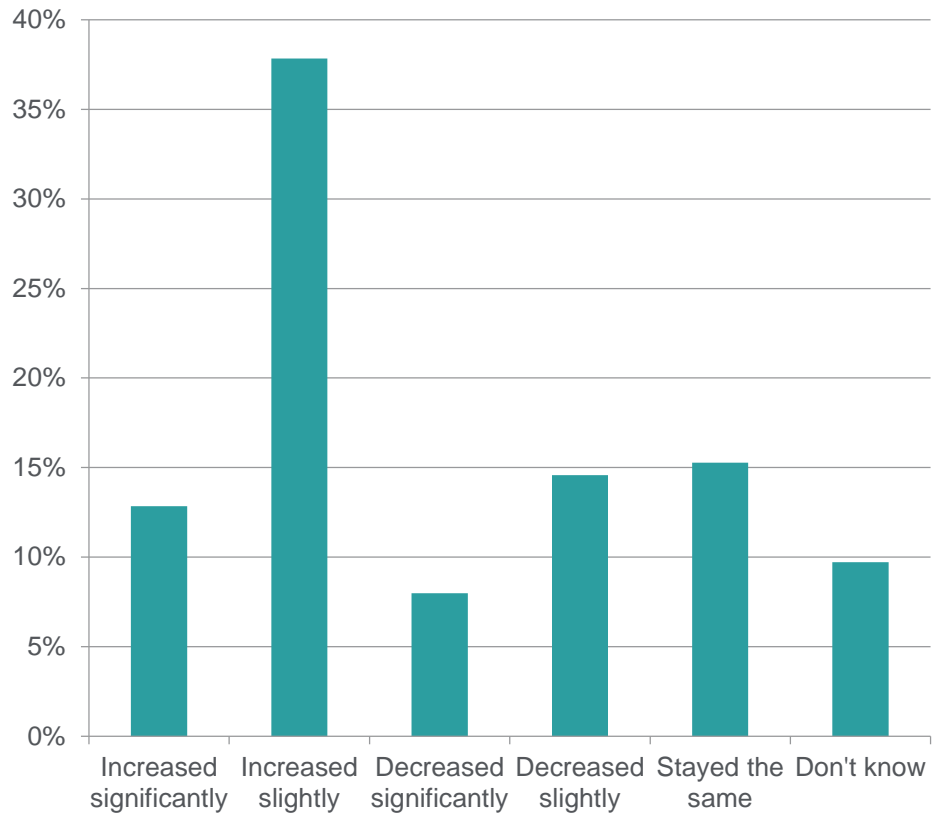


What are the biggest obstacles to writing cyber insurance policies? (select up to three)



Answer Choices	Responses	
Cost	42%	121
Scope of coverage	12%	34
Not understanding exposures	75%	215
Not understanding coverage	56%	161
Capacity constraints in market	6%	18
Application process	35%	101
Lack of value added products/services	7%	20
Different policy forms/coverages in market	26%	73
Answered		286

Coverage overlap between cyber and other policies has:

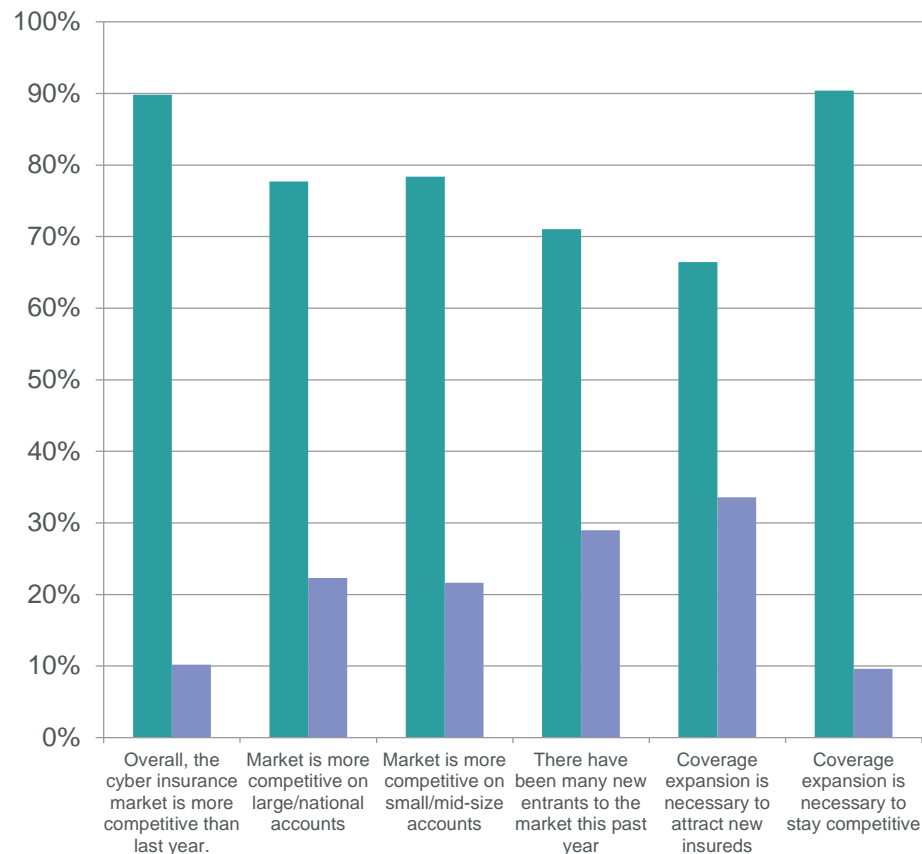


Answer Choices	Responses	
Increased significantly	13%	37
Increased slightly	38%	109
Decreased significantly	8%	23
Decreased slightly	15%	42
Stayed the same	15%	44
Don't know	10%	28
	Answered	288

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data

Please answer true or false to the following:

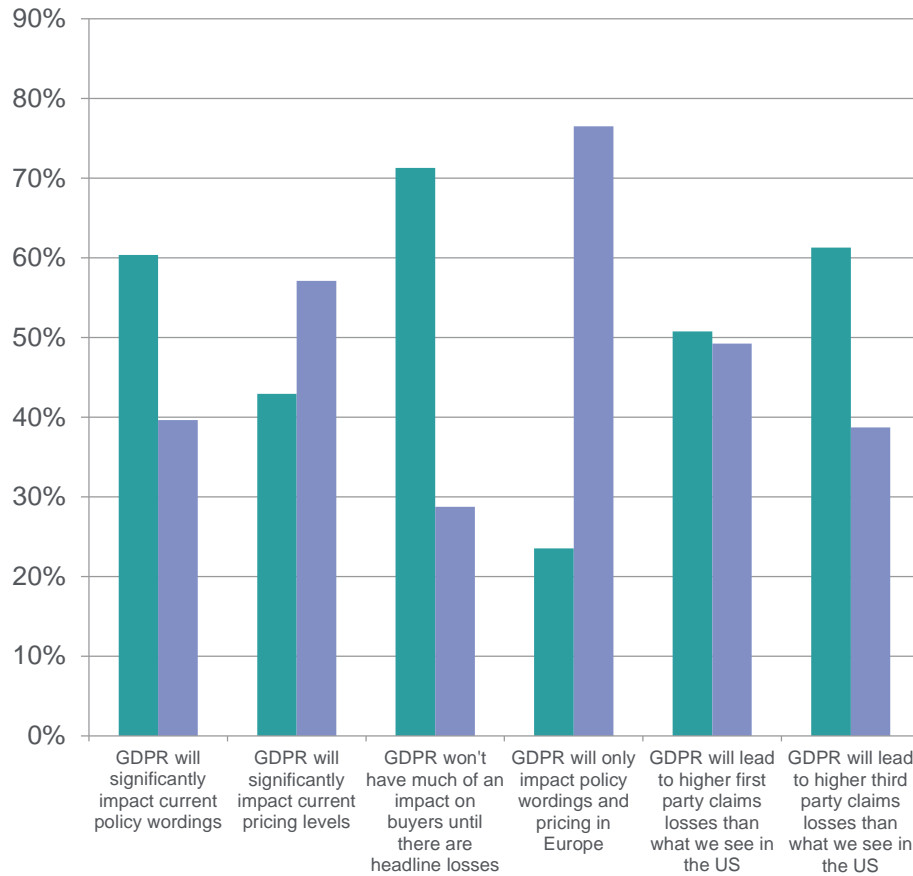


	True		False		Total
Overall, the cyber insurance market is more competitive than last year.	90%	256	10%	29	285
Market is more competitive on large/national accounts	78%	216	22%	62	278
Market is more competitive on small/mid-size accounts	78%	221	22%	61	282
There have been many new entrants to the market this past year	71%	201	29%	82	283
Coverage expansion is necessary to attract new insureds	66%	186	34%	94	280
Coverage expansion is necessary to stay competitive	90%	254	10%	27	281

2018 Survey of Cyber Insurance Market Trends

Supporting Raw Data

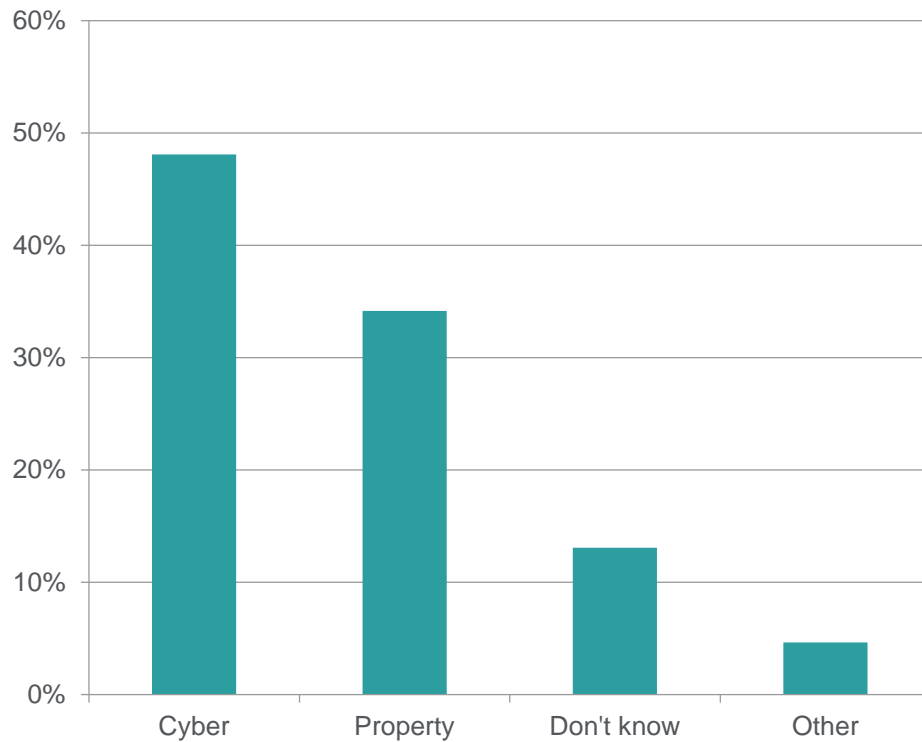
What do you think of GDPR? True or False.



	True	False	Total
GDPR will significantly impact current policy wordings	60% 163	40% 107	270
GDPR will significantly impact current pricing levels	43% 115	57% 153	268
GDPR won't have much of an impact on buyers until there are headline losses	71% 191	29% 77	268
GDPR will only impact policy wordings and pricing in Europe	24% 63	76% 205	268
GDPR will lead to higher first party claims losses than what we see in the US	51% 133	49% 129	262
GDPR will lead to higher third party claims losses than what we see in the US	61% 160	39% 101	261

■ True
■ False

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

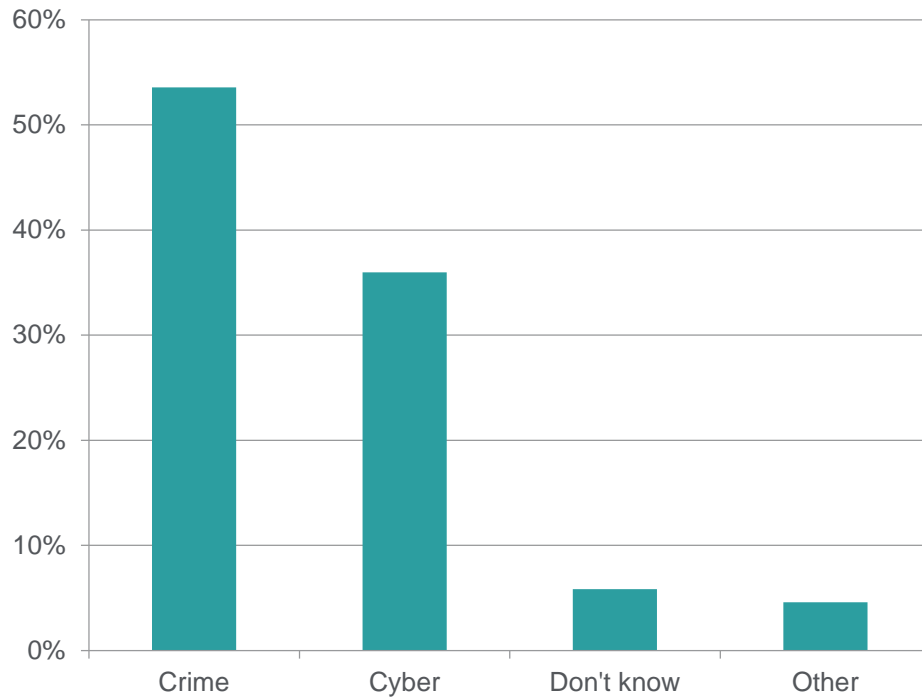


Question to brokers

Answer Choices	Responses	
Cyber	48%	114
Property	34%	81
Don't know	13%	31
Other	5%	11
	Answered	237



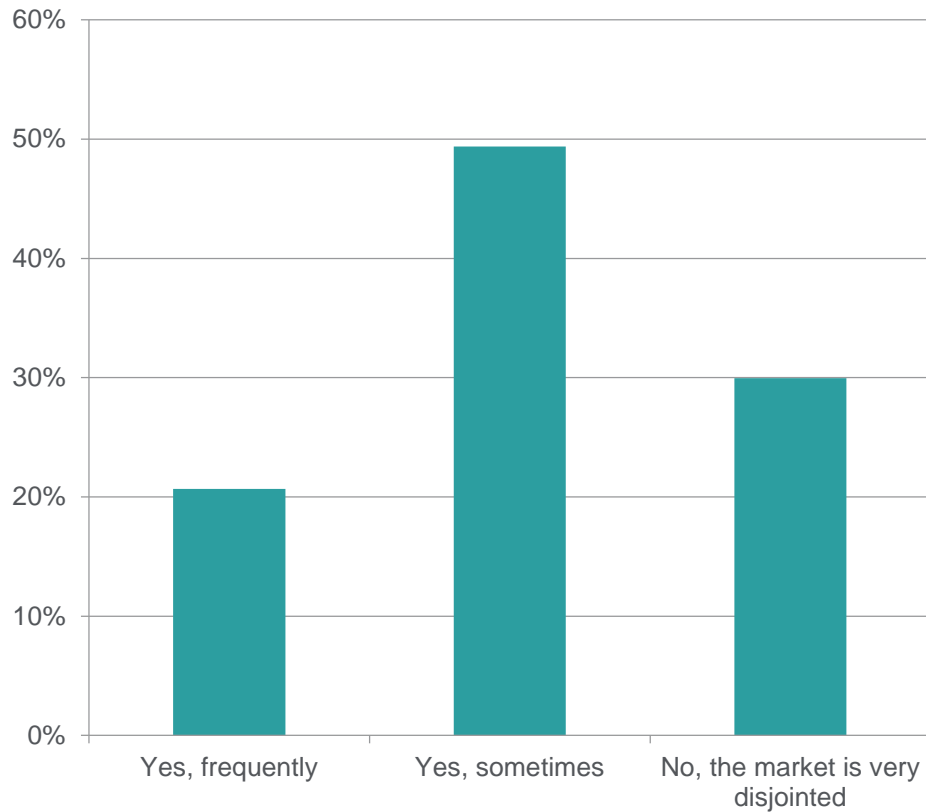
Do you believe funds transfer fraud loss due to social engineering fraud is better covered by a cyber policy or a crime policy?



Question to brokers

Answer Choices	Responses	
Crime	54%	128
Cyber	36%	86
Don't know	6%	14
Other	5%	11
	Answered	239

Is cyber insurance pricing becoming more consistent among carriers?



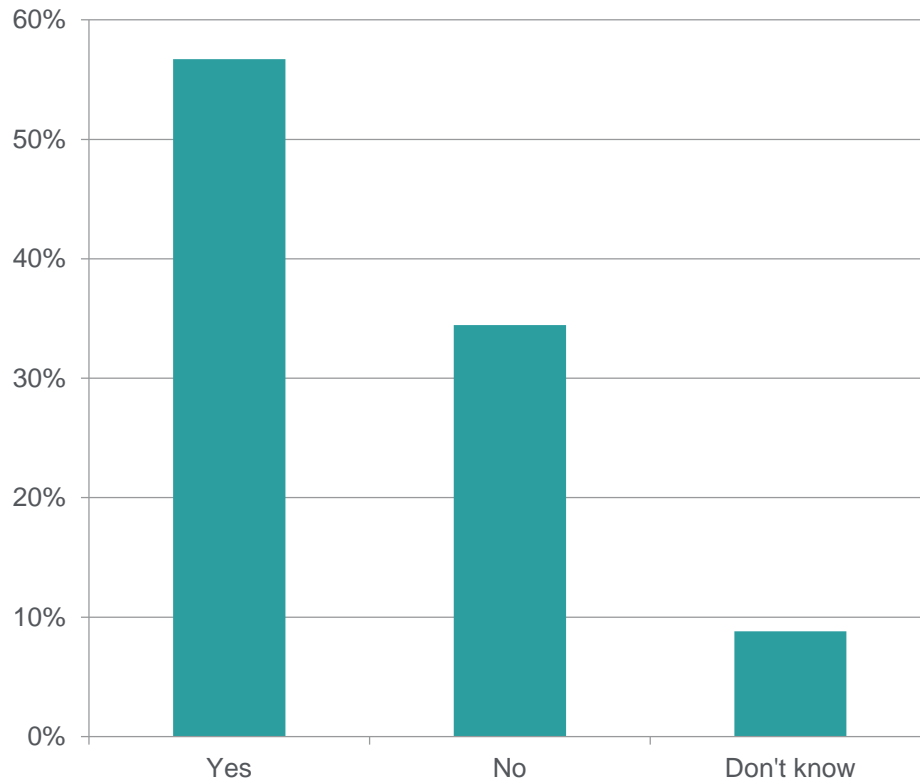
Question to brokers

Answer Choices

Responses

Yes, frequently	21%	49
Yes, sometimes	49%	117
No, the market is very disjointed	30%	71
	Answered	237

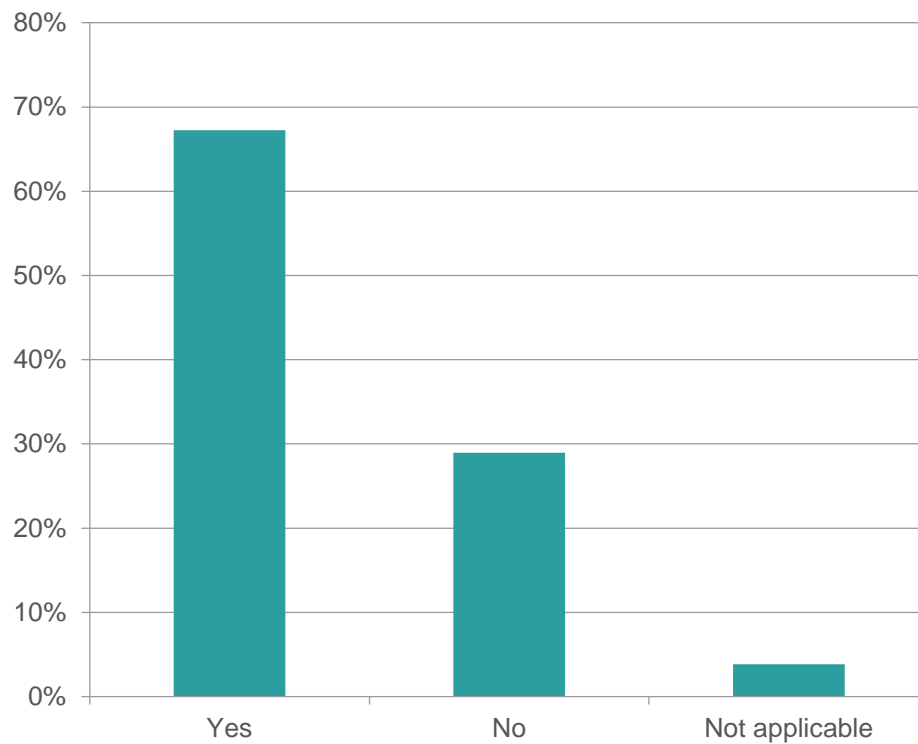
Is cyber insurance coverage becoming more consistent among carriers?



Question to brokers

Answer Choices	Responses	
Yes	57%	135
No	34%	82
Don't know	9%	21
	Answered	238

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

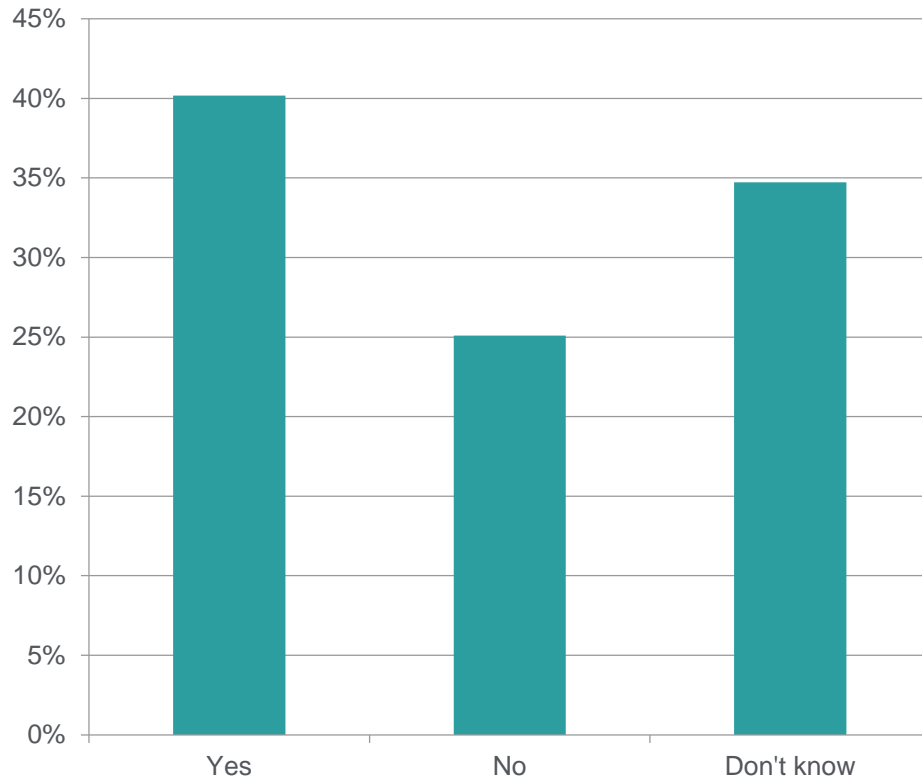


Question to brokers

Answer Choices	Responses	
Yes	67%	158
No	29%	68
Not applicable	4%	9
	Answered	235



Have you noticed a difference in claims handling among carriers?

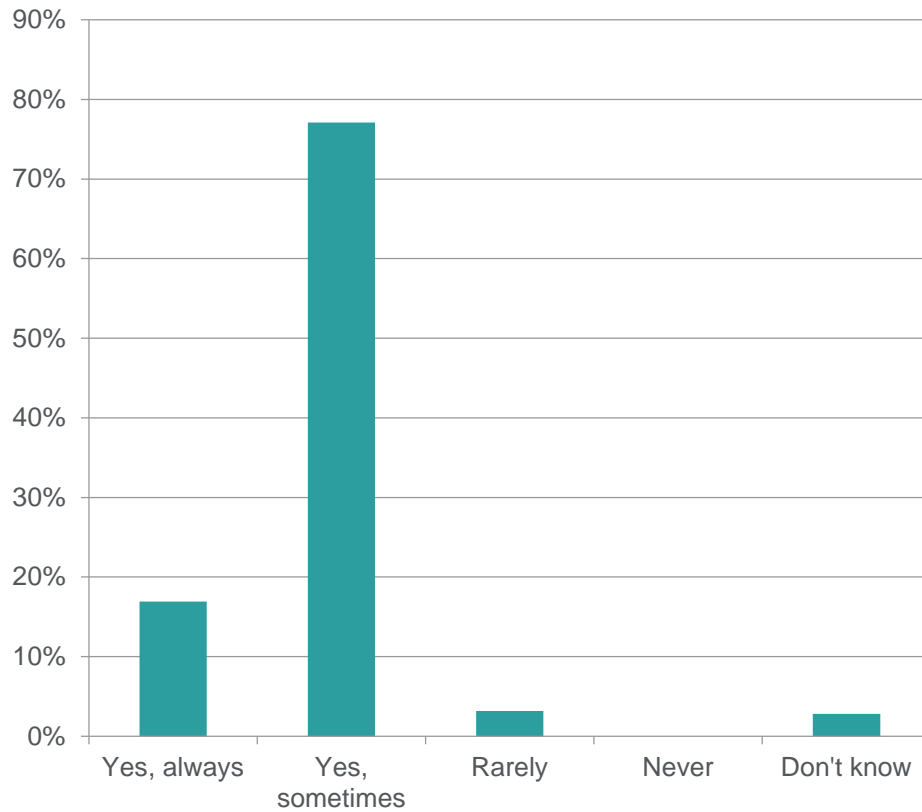


Question to brokers

Answer Choices	Responses	
Yes	40%	96
No	25%	60
Don't know	35%	83
	Answered	239



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



Question to brokers

Answer Choices	Responses	
Yes, always	17%	48
Yes, sometimes	77%	219
Rarely	3%	9
Never	0%	0
Don't know	3%	8
Answered		284

Slides 33 to 38 contain a selection of additional comments made by survey respondents. Please note, this content is included only as a point of interest and may not be reproduced or disseminated in any way.

Please add any comments or thoughts (positive or negative) you would like to share regarding the cyber insurance market:

Since all businesses have paper files, cell phones, laptops, computer terminals, web portals, it is almost impossible to avoid an exposure to data breach or cyber liability claims; cyber liability is an exposure that can't be retained or self-insured by small to medium sized companies

Cyber claims settlements are inconsistent among carriers. Courts are [inconsistent] with their settlements producing excessive costs for insurers and claimants alike. Contracts are all different and clients know this which contributes to their reluctance to buy cyber coverage

At times, insurance as a whole is looked at as a 'necessary evil' to conduct business. We need to provide clients products that are less restrictive (minimize exclusionary language) and will be able to respond to claims appropriately.

The application form and application process is still too difficult and takes too long for the client, especially the IT part, which is not understandable for the company manager.

Also there is the [lack] of cyber insurance coverage and understanding of [its] necessity for the client.

It always depends on the exposures, needs, and expectations of the insureds. Cyber exposures are continually expanding.

The market has evolved considerably in the past 10 years but all of the cyber coverages that were available(if you knew where to look) in 2011 are now being offered by a significant number of the leading markets - biggest changes include dropping prior acts and retro dates coverage exemptions, the development of BI and Contingent BI coverages, and cyber theft of funds - interestingly we haven't seen unanticipated causes of loss, nor an aggregated loss event, so the future remains.....uncertain ??

Speed of response is going to be a big differentiator in the future. Clients have expressed concern with Cyber Extortion wordings that require the insured to obtain approval from underwriters before paying as often demands come in after normal business hours with short timeframes. Having the individual taking the claim report able to advise and authorize (at least to a certain \$ amount) is going to be seen as a true advantage for these insureds.

There is an industry-wide need for carriers to revisit how they approach certain coverage extensions. No reason why a scenario may be covered under Cyber, Crime or Property policies. Like other loss, there should be 1 policy to address these issues. Once that is done then we can look for more consistency in policy language and definitions [as] terms vary significantly from carrier to carrier and pose challenges when reviewing and forming comparisons to clients.

Please add any comments or thoughts (positive or negative) you would like to share regarding the cyber insurance market:

I need more education. I watch as many videos and carriers as possible.
Capacity and accumulation risk with larger BI incidents at focus.
Requires clarity how the policy will respond in case of a claim. Cover different scenarios to help the insured understand the difference and importance of having a Cyber policy.
Cyber coverage for manufacturing systems is badly needed. Not the software which comes with a new piece of [manufacturing] equipment. Coverage for the many hours of customization done to each of these machines and their interface with engineering/design pc's.
Time will tell what the "right" price is for the breadth of coverage currently provided. It seems highly likely the premium for excess cyber coverage is not the "right" price.
Should be more linked to reinsurance concerns about systemic and CBI risks
Pre loss control is invaluable. Brokers have to push it onto clients. Until clients get hit, one can bring a horse to water, but one cannot make it drink.
More standardization required
The market is in a constant state of evolution, more reactive to technology change than anticipatory. Underwriters seem to lack overall expertise and ability to separate fact from fiction some days. More losses will help clarify that.
Needs to be more coordination of other insurance clause
Structural constraints remain a fundamental challenge to the industry. New exposures continue to emerge, the risk selection process is maturing and refinement is still needed in capturing the appropriate underwriting data. As an industry, we are working toward better risk differentiation – both in regard to structure offered as well as pricing discernment.
If you are going to layer limits you do not need to layer all coverage offerings in the primary.
The contract is specific to certain coverage generally Network Security, Regulatory or Privacy the rest do not need to be quoted for excess.
Reading and negotiating excess limits with client very important.
Reading and negotiating coverage with vendors even more important.

Please add any comments or thoughts (positive or negative) you would like to share regarding the cyber insurance market:

<p>In Brazil the market [is] very young, most carriers have no authority so the UW process is very slow. We are struggling with a lack of know-how on the side of UW and with a certain ignorance of the market. There's a lot of interest due to GDPR and Brazilian forthcoming LGPD.</p>
<p>Overall it is a new necessity for the market place, unfortunately, many businesses do not fully recognize their potential exposures and decline coverage until it is too late.</p>
<p>It remains difficult within many companies to get Finance, ICT and Legal aligned</p>
<p>As coverage terms continue to be refined and tweaked, the lengths that brokers and insureds need to go to in order to understand differences between coverage expansions is a major barrier to understanding the exposure. Claims example databases would be immensely helpful to illustrate such an esoteric loss exposure to buyers who are typically not computer/technology proficient.</p>
<p>More consumer education to the risk of cyber liability and exposures, specially small business.</p>
<p>The market needs to be more consistent on systems failure & breaches of insured's third party vendors & related business interruption. Furthermore, truly address social engineering fraud by working in conjunction with crime policies. Create premium discounts for policyholders that access & complete cyber risk management trainings via carrier resources.</p>
<p>I think that large businesses are aware of the risks surrounding cyber, but they also have the money to get protected and generally, they are less at risk because they have accurate security and IT team. The real problem is to get a startup or a small business with limited budget AND resources to accept to pay the related cyber premium. They don't see the risk.</p>
<p>So many business owners think the cyber coverage is necessary only when they "sell" on the internet or keep credit card information and until educated will resist buying cyber.</p>
<p>I understand markets have to be unique in offering coverages and stand out but cyber policies are all over the place and some consistency is required from carriers.</p>
<p>Agents need to be better educated on the options available and how to present to the client. Many times a class [is] presented by the carrier and they only present the options they offer</p>
<p>The current great results are misleading; pricing is based on historical where there have been low limits and limited coverage. We now have expanded limits and coverage and have yet to see the impacts of a large systemic event. System failure and CBI is sure to cause massive losses in the line.</p>

Please add any comments or thoughts (positive or negative) you would like to share regarding the cyber insurance market:

Cyber is certainly a growing and new product, hopefully the market won't give in and start adding contingent BI/PD to cyber policies, it just simply doesn't belong there. We write [mainly] med/mal, so a cyber incident resulting in the bodily injury of a patient would be covered under the medical professional automatically.

The US and European markets are different. Some clients prefer to consider the Cyber as an extension into their classic GL and/ or Property program, where the current Cyber policy available on the European market is considered as a new financial exposure with a dedicated protection. The underwriters have a limited experience in the assessment of the risk and we will probably see an increasing in the premium after big Cyber loss.

Coverage creep in a falling market is our greatest challenge. There will be a point where we need to think seriously about what best belongs in the cyber insurance market and what could be better dealt with and priced under other classes. Cyber insurance will need to re-find its core purpose.

There is huge opportunity for Cyber Insurance and related services in Africa but this remains untapped due to limited appetite by Underwriters and lack of awareness by clients.

Insureds don't understand exposure. Most agents don't understand coverage. Industry trying to turn cover into BOP endorsement to get some premium and some limited coverage. Recipe for a self-fulfilling disaster.

Higher need today among smaller companies and healthcare providers but they have to be convinced that they are vulnerable and better educated to purchase coverages

Cyber insurance will continue to be fluid since technology is constantly changing. I prefer non-admitted forms for that reason. I like to accommodate the needs of clients that have various exposures given their class of business and narrow my market consideration based on that.

The equally important aspect in buying a cyber insurance are the services attached to it, e.g. forensics, crisis management, legal assistance, etc. Our local insurers are offering this cover relying on the their [reinsurance]/capacity support (and perhaps treating it as an ordinary and generic lines like property, etc.) we need to see more primary insurers to likewise offer these services, not just capacity.

Surprisingly there are many agents out there that still do not offer this coverage to their clients. Big or small, all commercial accounts should consider cyber coverage to at least assist with 1st party exposures. It's the cheap sleep insurance for business owners.

Having worked in IT for 20 years and now consulting on cyber liability (which includes cyber policies), I think carriers lack an understanding of technology complexities, the most common (and likely) threats that would cause data breaches or business interruptions, and how technology is being used by businesses. Carriers seem to look at cyber as just another risk factor, but the speed and sheer volume of technology requires a new approach so coverages are pertinent, effective, and priced correctly.

Please add any comments or thoughts (positive or negative) you would like to share regarding the cyber insurance market:

The cyber insurance marketplace is extremely competitive at the moment, yet we're still seeing buyers reluctant to buy the coverage or increase the limits. I think that this is because of the fact that the losses simply aren't there and the coverage is still priced too high. I think this is supported by the number of new entrances to the market and the fact that rates are decreasing across all lines of business.

That being said, if there is a systemic event like AWS going down for 24 hours, I think the market could implode which is why prices aren't lower than they are. That being said, we haven't seen a system event since the blues got hit and even if a number of breaches of that size were to happen again, I don't think it would move the market given the amount of capacity out there. It would truly take a large cloud provider going down with BI losses across hundreds or thousands of insureds to move the market.

Cyber exposures are most of the time unknown by smaller companies until they get a loss. I'm not sure if insureds are receiving education on cyber or just don't want to spend time & money on protection they think they can do without. A considerable amount of insureds actually wanting cyber are ones that have gone through a loss.

The one thing that surprises me is how with all the talk about Social Engineering there is little to no feedback on Voluntary Parting of property by trick or scheme. We have been seeing some more claims in this area than traditional Social Engineering claims.

Emerging desire for exposures previously contemplated in the property insurance realm to be covered under Cyber policies could lead to the merging of those two lines of insurance in terms of offering, expertise, and headcount

There has been a lot of movement on the underwriting side, and so it seems like brokers are often working with new underwriters, many of whom do not yet have product expertise. This also means a lot of waiting on line underwriters to get approval on policy modification requests and premium negotiations. [In some markets], underwriter movement is a minor adjustment usually; [in other markets it] is another story entirely. Sometimes one or two underwriting leaders leaving [] has resulted in there being no remaining expertise to service existing placements or reliably quote renewal terms

Insurers are approaching cyber in the 2010's with the same approach as commercial package policies in the 1960's. That's resulted in a huge disconnected between customer needs and insurer offerings.

Previously focused on large enterprises, cyber insurance is now more attainable for SMBs who are requesting it more and are also being required to carry it as third party vendors.

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.

Need a combined cyber/crime coverage as too often it is difficult to see which policy should be covering.

Please add any comments or thoughts (positive or negative) you would like to share regarding the cyber insurance market:

I've been selling cyber insurance since 2014/2015 and this is the first year I have customers asking their agents for cyber quotes along with their professional liability renewals.

We have many excellent options, can easily get quick indications, especially for Small Business, and the pricing and coverage seems to be getting more competitive, but insureds are still hesitant to add another Insurance bill to their budget.

[Some markets] remains very aggressive, both in terms of price and coverage - e.g. willingness to extend Network Interruption coverage to cater for various stages in the supply chain remains in spite of the well-documented catastrophe risks (e.g. mass outages) and occasional lackluster underwriting information. Challenges in risk assessment remain for less sophisticated applicants - e.g. many struggle to provide a snapshot of the data they hold at a given point in time.

I think there is still confusion around social engineering vs crime vs cyber. AND Property damage vs Cyber. There seems to be more continuity in coverages offered such as media liability and business interruption but the definitions of those coverages varies vastly, e.g. Is print included? Limited to website or all electronic media? Definition of insured... etc.

News of Cyber Losses are driving buyer concerns.

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.