



US Cyber Market Update

2017 US Cyber Insurance Profits and Performance

July 2018

Introduction

WannaCry. NotPetya. Equifax. The continued explosion of ransomware. 2017 was an unprecedented year for cyber attacks. Cyber insurers found themselves responding to these events and sifting actual claims from fear, uncertainty, and doubt.

2017 is the year that cyber aggregation risk became real for many insurers. Ransomware, in particular, evolved the capability to spread instantly at the speed of connection, with a little help from the Shadow Brokers and NSA exploits. The NotPetya attack illustrated how software exploits could cause real-world disruption to the operations of multinational companies. Insurers found themselves potentially paying claims on multiple insurance lines, include property. Exploits are becoming intelligent and adaptive, powered by massive spam networks for phishing purposes. The new tactic is “infect first, then decide what to do about it.” At the same time, we saw Lloyd’s step up their attention to cyber risk, with the publication of papers specifically looking at the potential of systemic events primarily from common cloud service providers.

At Aon, we strive to understand how the headline-grabbing stories of 2017 actually translated into underwriting results for US cyber insurers. To that end, we are pleased to bring you the third edition of our *US Cyber Insurance Profits and Performance* study. We found that, despite the heightened worries of 2017, US cyber insurers appear to have had a very good year.

As in prior years, we draw our analysis from US NAIC statutory filings, now in their third year of reporting. Although this data set does have limitations and data quality issues (including, but not limited to, no inclusion of US business of non-US insurers and an incomplete picture of US insurers with non-US business), we aim to take its general lessons as representative of US industry experience. See the “About the Data” section at the end of this paper for a full discussion of our approach to addressing these issues.

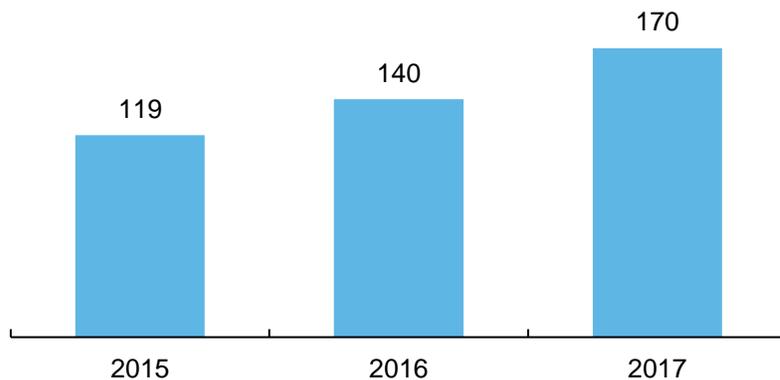
The US cyber insurance market continues to grow. A total of 170 US insurers reported having underwritten cyber insurance in 2017. Aon has analyzed these filings and shared our key findings on the following pages. Our aim is to provide insights for insurers that currently offer cyber insurance, as well as those seeking to offer it, to provide a performance benchmark, and to give perspective on the industry experience.

Key Findings on 2017 US Cyber Insurance Performance

Premiums and market participation are growing

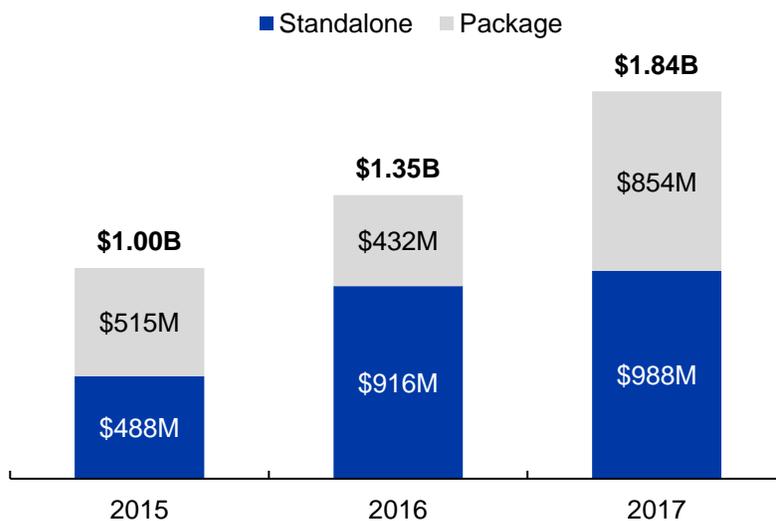
A total of 170 US insurers reported direct cyber written premium to the NAIC in 2017, up from 140 in 2016. The new market participants averaged \$140,000 in premium each. Also, note that these numbers do not include MGAs.

Exhibit 1: Number of US cyber insurers | 2015 – 2017



US cyber premiums grew to \$1.84 billion in 2017, a 37 percent increase from the prior year. Most of the growth came from package business, where premiums rose 98 percent year on year. Standalone cyber premiums grew 8 percent. We did observe that a number of insurers, including Chubb (#1 by total cyber written premium in 2017), reported decreases in standalone premiums offset by significant increases in package business. It is unclear whether the numbers in fact reflect more bundling of technology E&O and cyber risk together or simply a reclassification of policies that were previously considered standalone.

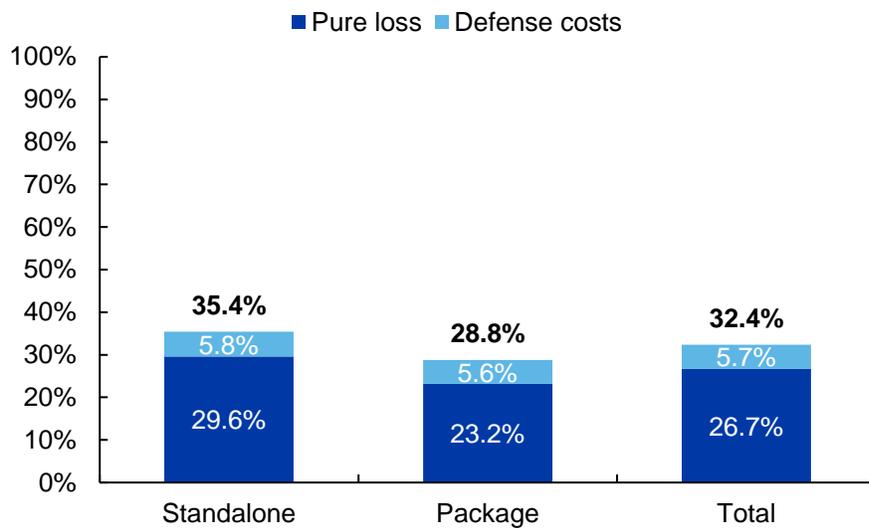
Exhibit 2: US cyber direct written premiums | 2015 – 2017



Loss ratios improved in 2017 for most insurers

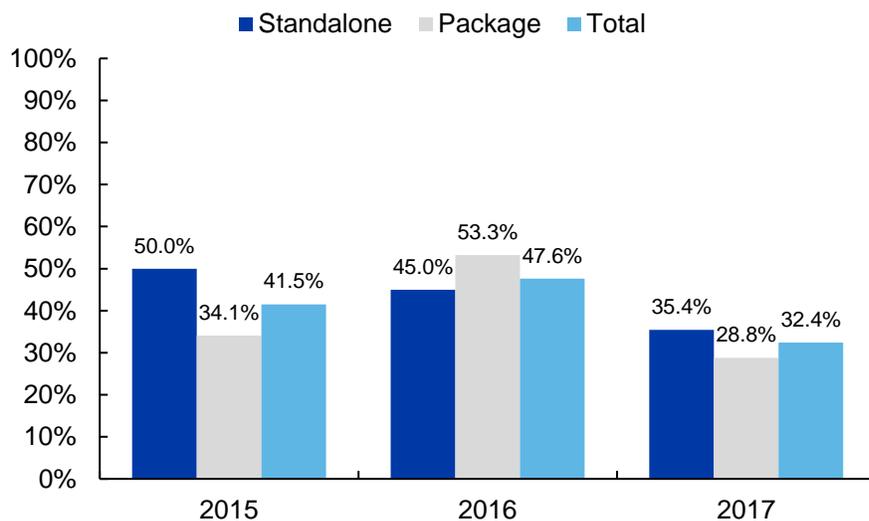
By most accounts, 2017 was a very good year for US cyber insurers, despite the headlines garnered by WannaCry, NotPetya, and Equifax. The direct incurred industry loss ratio was **32.4** percent across all policies, with standalone and package business reporting 35.4 percent and 28.8 percent respectively.¹

Exhibit 3: US cyber loss ratios | Standalone vs. package



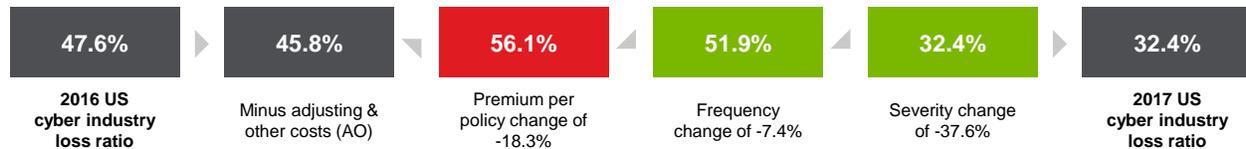
These numbers are a noticeable improvement from 2016, when the industry loss ratio was 47.6 percent. However, in 2015 and 2016, the NAIC also included adjusting and other expenses in loss ratios, whereas they did not in 2017. Adjusting and other costs averaged 1.7 loss ratio points in 2015 and 2016 – a minor component of the loss ratio but one worth noting.

Exhibit 4: US cyber loss ratio | 2015 – 2017



We found that the 2017 loss ratio decrease was primarily due to a reduction in claim severity. The average 2017 claim size across all companies was \$56,688, down from \$90,865 in 2016. This drop in severity, combined with a modest reduction in frequency, more than offset a reduction in the average premium per policy. This drop in premium per policy reflects the shift from standalone business to package business, at lower per-policy prices. (Premium per policy increased on both a standalone and package basis, respectively.)

Exhibit 5: Components of Loss Ratio Change, 2016 to 2017



In light of the headlines that cyber attacks garnered last year, this reduced loss ratio may seem surprising. Here are several considerations that may help explain the result:

- The NAIC is collecting losses on a calendar year basis, not accident year or policy year. The 2017 numbers are impacted by changes in reserves from earlier accident years. We know of at least one large insurer whose 2017 reported results were reduced by prior year reserve releases.
- Small commercial insureds are a growing portion of the overall cyber market. Small companies purchase smaller limits, their incidents are less costly to remediate, and, according to Aon's analysis of Advisen data, small companies are less targeted on a per-company basis by cybercriminals than large companies. We have observed better loss ratios for small-medium enterprise (SME) focused insurers than the market overall. As this segment grows, it may be bringing down severity and loss ratios overall.
- Ransomware continues to grow as a favored attack method for cybercriminals. As a result, we are seeing a broad shift from attacks on large single data repositories, such as Target and Equifax, toward numerous small attacks on data in the hands of many different individuals and businesses. These small attacks have been broadly automated by cybercriminals, meaning the attacks are almost frictionless to carry out. While the take-up rate of cyber insurance is high for large US businesses, it is much lower for individuals and small businesses. As a result, the growth of ransomware is likely causing a shift toward victims who are not currently insured by the US cyber market.
- This increase in ransomware may also have implications on frequency and severity. Decreases in severity were observed in both standalone and package business. However, an increase in frequency per policy was observed in standalone business (offset overall by the shift toward package). The rise of ransomware may result in more frequent, but less severe, claims.

That said, by comparing loss ratios a different way, we received mixed messages about insurers' profitability in 2017 versus 2016. Here, we segmented insurers based on the magnitude of their loss ratio change from 2016 to 2017, looking only at writers with at least USD 5 million in direct written premium to avoid potential skewing from small premium bases. A change of at least 5 loss ratio points was selected to indicate a material change. The results appear in Exhibit 6.

Exhibit 6a: US cyber loss ratios, 2016 vs. 2017 | Standalone policies

For insurers with direct written premium greater than USD 5 million

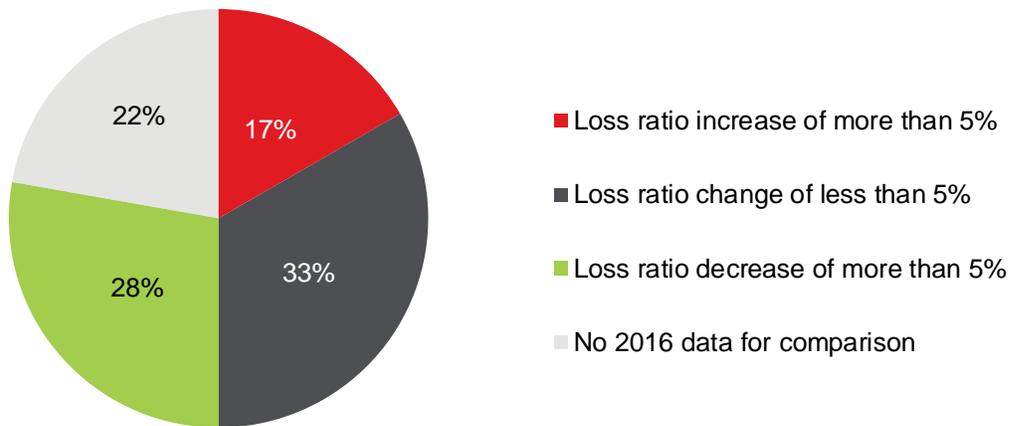
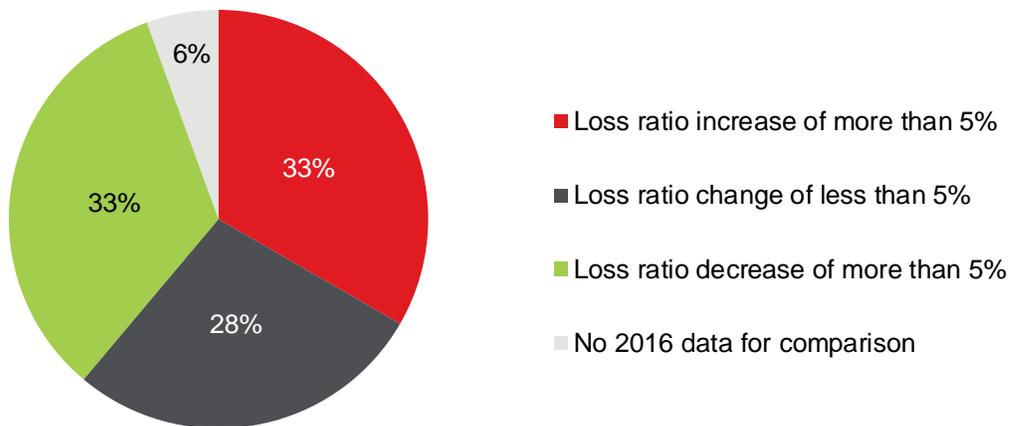


Exhibit 6b: US cyber loss ratios, 2016 vs. 2017 | All policies

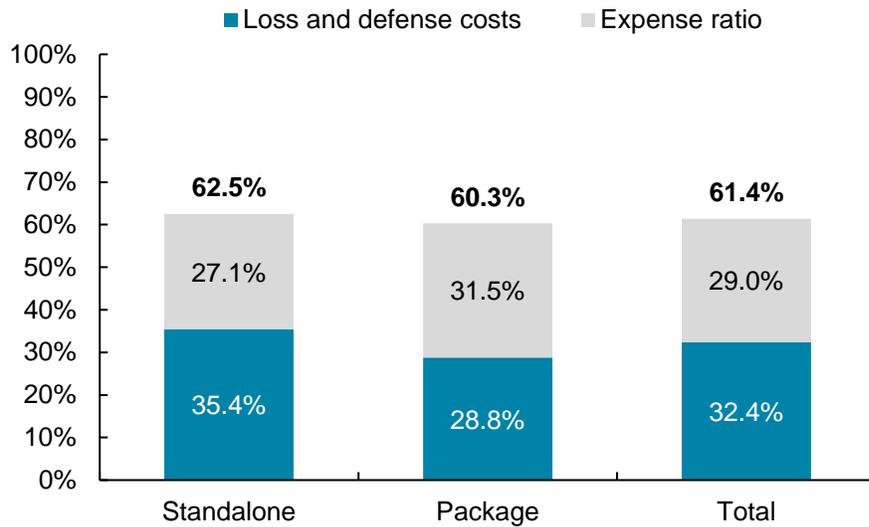
For insurers with direct written premium greater than USD 5 million



These charts indicate that for standalone cyber, notably more insurers saw decreases in loss ratios than increases in loss ratios, 28 percent versus 17 percent. But when examining all cyber premiums including package, the results are mixed. On examining the data more closely it appears that all of the top 5 package cyber insurers experienced loss ratio decreases—many of them significant—but a number of smaller package insurers saw loss significant loss ratio increases. This may reflect economies of scale and the development of claims handling expertise that the largest cyber insurers have been able to develop.

Finally, we estimated the industry's cyber combined ratio for 2017, using expense ratio estimates from the Insurance Expense Exhibit.² The result appears in Exhibit 7 and further illustrates the profitability of US cyber insurance in 2017.

Exhibit 7: Estimated 2017 US cyber combined ratios



Volatility increased slightly among insurers in 2017

Individual insurers saw loss ratio results both higher and lower than the average of 32.4 percent – some notably so. Among underwriters with at least USD 5 million in direct written premium, loss ratios ranged from zero percent at the low end to 223.7 percent at the high end.

The coefficient of variation (CV) of insurer loss ratios – defined as the standard deviation divided by the mean – rose modestly in 2017.

Exhibit 8: Coefficient of variation of direct loss ratio by year

Calendar Year	Insurers with > USD 5M	Insurers with > USD 50M
2016	104.3%	55.9%
2017	116.1%	58.7%

A single outlier can significantly influence these volatility metrics. To look at the data a different way, we also look at the percentile distribution of loss ratios for insurers. The table below shows the range among insurers with more than USD 5 million in written premium.

Exhibit 9: Cyber insurance loss ratio percentiles by year

Calendar Year	5th Pctl	25th Pctl	Median	75th Pctl	95th Pctl
2016	0.4%	5.3%	20.5%	51.2%	92.7%
2017	1.9%	5.4%	25.5%	45.8%	79.3%

We do see large loss ratios in the data, as seen from the 95th percentile result of 79.3 percent. Also, the median for 2017 is higher than for 2016, 25.5 percent versus 20.5 percent.

For insurers providing cyber insurance, these results illustrate the potential for both good *and* extremely bad underwriting outcomes and underscore the importance of managing limits. It appears that most

insurers were minimally affected by the events that grabbed headlines in 2017. We note that WannaCry and NotPetya primarily affected companies outside the US.

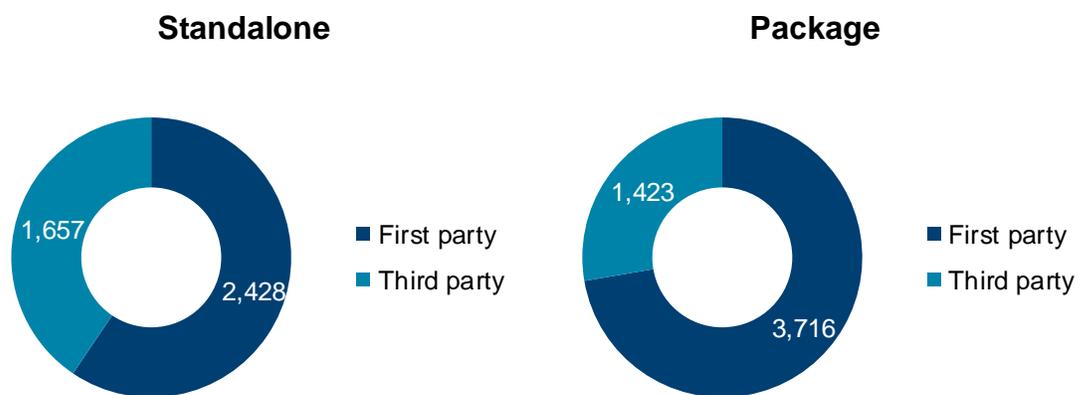
First party claims predominate

In 2017, claims against first party coverage outnumbered third party claims, accounting for two-thirds of all claims. For standalone policies, first party claims made up 59 percent of the total, while for package policies, first party was 72 percent of the total. The claim results are summarized below.

Exhibit 10: US 2017 cyber claims

Total Claims: 9,224

Total First Party Claims: 6,144 | Total Third Party Claims: 3,080



This is consistent with what we hear from conversations with our clients, with first party claim costs accounting for most of what insurers are paying.

Claims rates were significantly higher for standalone business. Cyber claims occur at a rate of 3.9 per 100 standalone policies, versus a rate of 0.2 per 100 package policies. Remember that “package” business may vary in meaning for different insurers, ranging from cyber endorsements on small commercial or BOP policies to large cyber / technology E&O blended policies.

Premiums are growing and the field is widening

In 2017, US cyber premiums grew approximately 37 percent year on year to USD 1.84 billion.

As we expected to see, a growing number of insurers participated in the US cyber market in 2017, reducing the market share held by the largest players. In total, 170 insurers reported writing some cyber premiums in 2017, with 37 insurers writing premium in 2017 that did not in 2016. 79 insurers wrote more than USD 1 million and 36 wrote more than USD 5 million. All these numbers are higher than in 2016. The largest growth occurred among insurers with less than USD 1 million in premium. These were mainly writers of package business, which contributed to the observed growth of package premium in the market.

The top five cyber insurers accounted for 51 percent of direct written premiums, down from 52 percent last year, and the top 10 accounted for 69 percent versus 73 percent last year. By way of comparison, the top 10 writers of other liability claims made insurance account for 57 percent of premium and the top 10 in commercial multi-peril account for 44 percent of premium.³ The US cyber market is still relatively concentrated, but less than before due to the participation of new entrants.

The charts below illustrate the distribution of cyber premium.

Exhibit 11: US 2017 cyber premium distribution by size rank
Total premium reported: USD 1.84 billion

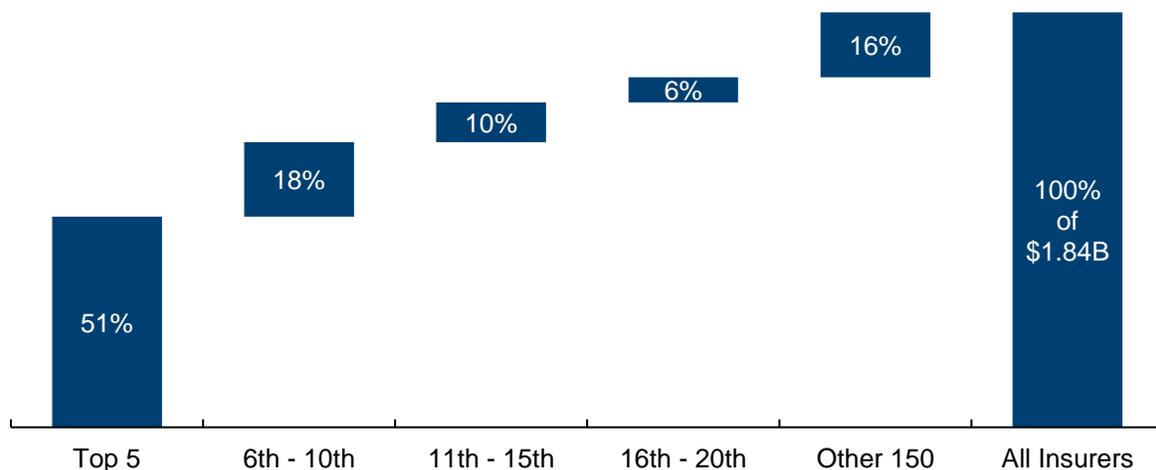
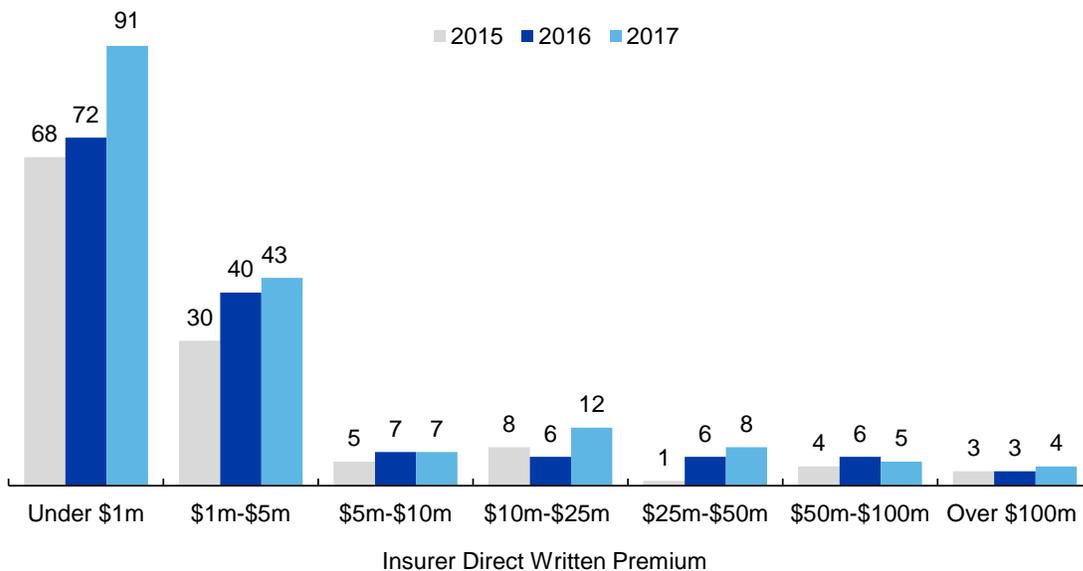


Exhibit 12: Number of US cyber insurers by direct written premium



About the Data

The NAIC supplement requests insurers to report on several kinds of coverage:

- Standalone cyber insurance policies
- Cyber insurance that is part of a package policy
- Standalone identity theft insurance policies
- Identity theft insurance that is part of a package policy

For our analysis, we have focused on the cyber insurance coverages, both standalone and package.

For this year's study, the data was extracted on June 4, 2018.

We looked to extract as many insights from the supplement data as possible, but have some concerns about the completeness and quality of the reported information. We suggest reading this briefing not as commentary about the US cyber industry per se but rather as commentary about *this particular dataset*. We have commented on anomalies in the data where we are able to identify and adjust for them. We discuss a few specific data issues on the next page.

Premium completeness

Our analysis suggests that the data reported to the NAIC is only a partial picture of the US cyber insurance market. London and Bermuda insurers also provide coverage for US risks, and those premiums are not reflected in this data. The NAIC data represents a sizable portion of the US market but is not comprehensive. Additionally, the NAIC data not reflect the entirety of the performance of US insurers that write internationally.

Issues with package policies

The treatment of cyber package policies creates several issues worth noting, particularly when comparing results against standalone policies:

- Premiums for the “cyber” portion of package policies can be difficult to break out. About 14 percent of the total package cyber premiums reported are from insurers who were unable to quantify the amounts exactly and instead used estimation techniques.
- Losses reported for package policies do not include IBNR. The NAIC requested payments and case reserves for package policies, whereas it requested payments and total incurred amounts for standalone policies. It remains unclear whether insurers interpreted the standalone “incurred” losses to include IBNR. But the results for package business clearly do not.
- Insurers were left to interpret the meaning of “package” business for themselves. “Package” in cyber can be interpreted extremely widely, ranging from an endorsement on a small commercial or BOP policy to a large cyber / technology E&O blended policy. We see this in the policy counts for package insurers: a number have more than 100,000 policies issued, while others with fewer than 20,000 are collecting significantly more premium. Thus, the results for package business are less homogeneous than the results for standalone cyber.

Claims data quality

Not all insurers reported cyber claim counts, and of those that did, the number of claims varied considerably. The mix between first and third party claims also varied significantly between some insurers. We analyze the data on a per-claim basis only with a measure of caution.

Contact Information

Authors

Jon Laux, FCAS

Head of Cyber Analytics
Aon Benfield
+1 312 381 5370
jonathan.laux@aonbenfield.com

Craig Kerman, FCAS

Director, Cyber Practice Group
Aon Benfield
+1 212 441 1568
craig.kerman@aonbenfield.com

Alexa Yakely

Analyst, Cyber Practice Group
Aon Benfield
+1 212 441 2681
alexa.yakely@aonbenfield.com

Aon Benfield Cyber Leadership

Catherine Mulligan

Cyber Practice Group Leader
Aon Benfield
+1 212 441 1018
catherine.mulligan@aonbenfield.com

Luke Foord-Kelcey

Cyber Practice Group Leader
Aon Benfield
+44 (0)20 7086 2067
LFK@aonbenfield.com

Sources:

¹ Company calendar-year loss ratios weighted by direct earned premium. All numbers reported to the NAIC are on a direct basis.

² 2017 Insurance Expense Exhibit. Based on a premium-weighted average of the other liability-claims made expenses (for standalone cyber premiums) and commercial multi-peril liability expenses (for package premiums).

³ Source: NAIC 2017 statutory filings, as captured in S&P Global Market Intelligence as of June 4, 2018.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

© Aon plc 2017. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

About Aon

Aon plc (NYSE:AON) is a leading global professional services firm providing a broad range of risk, retirement and health solutions. Our 50,000 colleagues in 120 countries empower results for clients by using proprietary data and analytics to deliver insights that reduce volatility and improve performance.

© Aon plc 2018. All rights reserved.

The information contained herein and the statements expressed are of a general nature and are not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information and use sources we consider reliable, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.