ABConnect

Reinsurance

Disruptive Technology - Cyber

Silent Cyber Scenario: Opening the Flood Gates

Jon Laux
Managing Director with Aon's Reinsurance Solutions business and Global Head of Cyber Analytics

Matthew Honea
Director of Cyber at Guidewire/Cyence

Click here to view the printable version

Over the past few years, cyber risk has moved from imagined scenarios to become a threat that is increasingly real and prevalent.

Cyber insurance products are growing quickly, but at roughly USD 4 billion in premiums they comprise less than 0.3 percent of the global property-casualty market. The greater concern for the insurance industry is the potential “silent cyber” risk residing in traditional property and casualty policies—this is the risk that a cyber event could trigger unexpected payouts under existing policy wordings.

Concerns about silent cyber risk are not unfounded. In December 2015, Ukraine experienced widespread power outages lasting about six hours due to malicious code. A further malware attack in 2017 caused widespread disruption to services throughout Ukraine, and spread to certain U.S. and European multinational companies operating there. This attack – referred to as NotPetya – generated claims both on property and affirmative cyber insurance policies. In mid-2018, an evolved version of the malware used against the Ukrainian power grid has successfully infected critical infrastructure in Eastern Europe. The level of sophistication behind this new malware – dubbed GreyEnergy – suggests that critical infrastructure remains both targeted and vulnerable.

Recognizing the potential for a cyberattack to cause potential physical damage and insurance claims in the U.S., Lloyd’s of London and Cambridge University published a widely read report on the potential consequences of a hypothetical attack on the Northeastern U.S. power grid, which include

insurance claims spanning property, general liability, management liability and other policies. Other areas of critical infrastructure are also at risk but have been less scrutinized than power generation. In this paper, we create silent cyber scenarios in which a cyberattack on a hydroelectric dam in the United States impacts local businesses and homeowners.

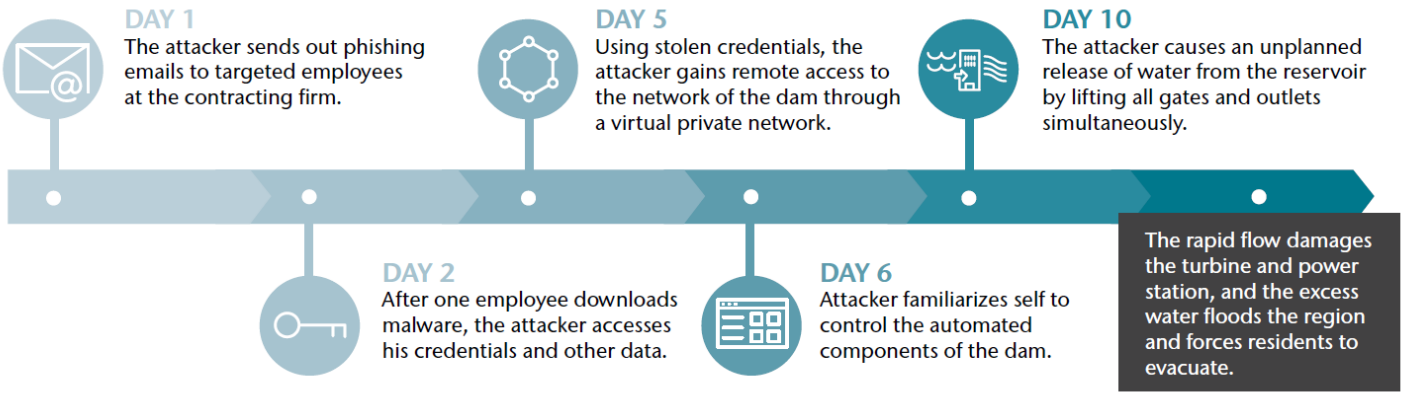
There are over 90,000 dams in the U.S., serving purposes including irrigation, hydroelectric power, flood control, and recreation. With the vast majority—93 percent—being owned and operated by state and local governments and private companies, most U.S. dams are not tightly regulated for cyber-security. Yet dam operators are increasingly automating control systems, both to realize efficiencies and to capture real-time data that improves dam safety and operation. While automation certainly has benefits, it also creates new risks. In 2013, an Iranian national, Hamid Firoozi, successfully breached the control system of a dam in Rye Brook, New York. Firoozi could have remotely operated the dam's gate if Rye Brook's electronic gate controls had not been taken offline for maintenance at that time.

Furthermore, recent assessments by the Department of Homeland Security and the Office of the Inspector General have highlighted poor security practices including weak network segmentation and access controls.

Dam Attack Scenarios

In these scenarios, a threat actor seeks to create massive disruption in the U.S. by causing flood damage. The threat actor identifies an engineering firm that has been contracted to support the IT systems at a hydroelectric dam, and through carefully crafted phishing emails, gains access to the engineers' system. Once in the engineers' network, the threat actor waits for an engineer to log in remotely to the dam's control systems and captures their login information. The threat actor then uses these credentials to access the system.

After several days of reconnaissance in the control system network, the threat actor has learned the commands used for the dam operations, including the controlled release of water by raising the gates and outlets. At this point, the threat actor executes a command to raise all gates and outlets to maximum height, causing an uncontrolled and unscheduled outflow of water. This sudden outflow damages the turbines at the hydroelectric power plant, as well as causing rapid and massive flooding downriver to homes and businesses.



Damage Impact to Insurers and Society

We analyzed the potential impacts of the scenarios at three U.S. dams, selected to reflect small, medium, and large exposure value, respectively. The dams have potential cyber exposure due to their use of technology and industrial control systems (ICS), and demonstrate a range of damage levels that could occur from a cyberattack.

(We acknowledge that this analysis is not exhaustive; while these dam structures may be representative of the water and wastewater sector at large, we excluded several potential complicating factors—loss of life, negative health effects, agricultural impacts, the breach of multiple dams in the same water system or that use the same IT contractors—from the model for the sake of simplicity.)

Characteristics	Dam 1	Dam 2	Dam 3
Construction type	Earth and rock fill embankment dam	Earth and rock fill embankment dam	Concrete gravity dam
Reservoir capacity	180,000,000 m^3	4,400,000,000 m^3	1,205,000,000 m^3
Floodplain population	115,000	170,000	695,000
Exposed value	$34.5 billion	$37.3 billion	$200.8 billion

If one of these scenarios were to occur, it would likely result in property, liability, and affirmative cyber insurance losses for the dam operator. For purposes of this study though, we are focusing on the much larger potential impacts resulting from downstream flood damages.

With a team of flood modeling experts, we estimated economic and insured losses for both residential and commercial properties. Our key findings were that a cyberattack would cause:

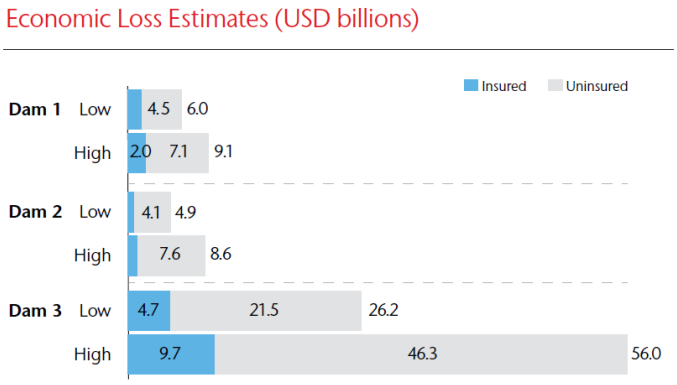
- Major impacts not only to dam operations but also to the resilience of local businesses and communities, with the highest economic loss estimated at USD 56 billion,
- Silent cyber exposure to insurers, with total insured losses of up to USD 9.7 billion, and
- A significant protection gap that would hurt homeowners and businesses if such an event were to occur, with only 12 percent insured in one of the dam scenarios.

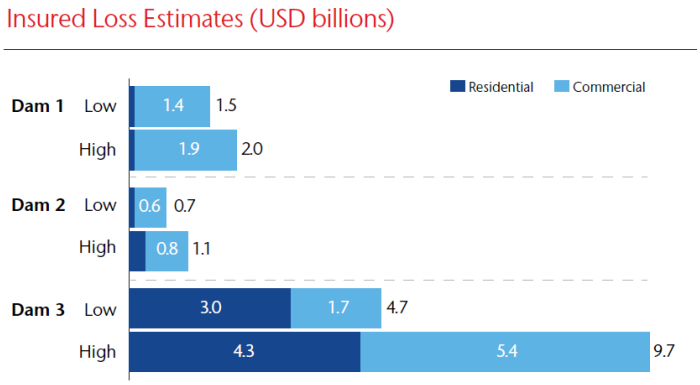
With up to USD 56 billion of economic loss estimated for Dam 3, these numbers certainly illustrate the potential damage from a cyberattack causing a flood.

Note that while Dam 3 shows the highest severity, this does not necessarily imply that it would have the lowest frequency. A threat actor looking to cause disruption to the U.S. would seek to cause the most extreme impacts possible - such is the nature of man-made catastrophes. As a result, the peril of cyber risk may actually "inflate" the tail or increase the likelihood of extreme events relative to what safety experts and flood modelers would expect to see from natural disasters and accidental failures.

One striking finding is that in all the scenarios, the majority of the loss is uninsured. This is due to low take-up rates of flood insurance, which we will discuss in more detail below.

The losses that are insured are comprised of residential and commercial properties, with residential losses flowing almost entirely into the National Flood Insurance Program (NFIP). NFIP losses could range from negligible to approximately USD 4.4 billion on the high estimate for Dam 3. Commercial insurance losses range from USD 585 million up to USD 5.4 billion across the three dam variants.





Silent Cyber Implications

We define "silent cyber" exposure as the potential for cyber risk to trigger losses on policies where coverage is unintentional, unpriced, or both. "Unintentional" coverage means not explicitly excluded or affirmed (with any applicable sublimits). Flood policies have unintentional cyber risk because the proximate and covered cause of loss would be the flood— not the cyberattack causing the flood. Similarly, flood policies will not have priced for a rise in flood frequency or severity as a result of cyberattacks. As a result, we conclude that both residential and commercial flood policies will generally have silent cyber risk.

Protection Gap Implications

Although private insurance and the NFIP would each take a share of the loss, the vast majority of loss from these scenarios would remain uninsured. We estimate that of the homeowners affected, very few would have flood insurance, as areas downstream of these dams mostly fall outside of FEMA Special Flood Hazard Areas and take-up of flood insurance outside of those areas is extremely low. We also anticipate many businesses will lack coverage—particularly small businesses, where flood protection is not commonly part of property policies and must be purchased separately, typically from the NFIP. If such a cyberattack were to occur, it would further illustrate the significant protection gap that exists for flood risk in the U.S.

Reinsurance Implications

Generally, affected insurers would have protection from their reinsurers in these scenarios. Property reinsurance treaties provide for direct physical loss—which in these scenarios occurs as a result of a cyberattack. Often, this treaty protection is for named perils, so insurers should ensure that flood is on the list. Cyber-enabled flood damage could also have implications for reinsurers of the NFIP. In the scenarios for Dam 3, reinsurers would be exposed to loss.

Conclusion

These scenarios were created to illustrate how technology and connectivity, while generally seen as beneficial, could have unforeseen and undesirable consequences for businesses and homeowners, and by extension their insurers. Businesses must consider the security risks that new technologies could introduce into their environment, including potential impacts on their clients and communities.

Insurers must also consider how changing technologies can cause "established" perils such as flood to morph into new risks, with resulting changes to frequency and severity. By using scenarios such as these, insurers have the ability to stress test their portfolios against new and emerging perils created by cyber risk. With that knowledge, insurers can take steps to mitigate risk, through reinsurance as well as working with businesses to increase their resilience.

Lastly, we hope this paper draws additional attention to the importance of closing the protection gap as flood risk causes harm to society in the U.S. and around the world.

Learn More

For a detailed review of these scenarios, including key assumptions, additional loss detail, and deeper exploration of the cyber risks affecting critical infrastructure, access the full report at http://bit.ly/cyber-dam-scenario-report-2018.

A reference list is available in the full report.

About the authors

This report was a collaboration with the Cyence Risk Analytics product team at Guidewire.

Jon Laux is a managing director with Aon's Reinsurance Solutions business and global head of Cyber Analytics. Jon leads a global team of actuaries, consultants, predictive modelers and experts in catastrophe risk focused on helping insurers to grow in cyber insurance and to manage cyber risk effectively through the development of leading edge analytical tools, business intelligence, and advisory services. This team manages the development of Aon CyberMetrica, our probabilistic model for quantifying cyber accumulation risk. He is a Fellow of the Casualty Actuarial Society.

Matthew Honea is the Director of Cyber at Guidewire/Cyence who has worked extensively in the areas of threat intelligence, network defense, system forensics and discovery, enterprise security auditing, malware analysis and physical security.

Other major contributors to this article include Dr. Yoshifumi Yamamoto, also part of the Cyence Risk Analytics team at Guidewire, and Craig Guiliano and Dr. Megan Hart at Aon.

Aon
Cyber

US Cyber Market Update

2018 US Cyber Insurance Profits and Performance

June 2019

Empower Results®

Introduction

We are pleased to bring you the fourth edition of Aon's *US Cyber Market Update*, covering the industry's 2018 performance. In the four years of our study, we have seen reported premiums for US insurers more than double, from USD993 million in 2015 to over USD2 billion in 2018. Cyber insurance has been profitable for the large majority of insurers, in spite of the industry seeing cyber catastrophe losses from NotPetya in 2017. Of course, most insurers remain much more concerned about the potential for aggregating losses yet to come – whether they manifest as affirmative cyber market losses or, more broadly, claims in traditional property-casualty lines arising from silent cyber exposure. At Aon, these are risks we are watching closely.

But the main cyber story of 2018 is arguably the lack of a story: US insurers are not growing at the pace they were previously. Certainly, it can be challenging to maintain annual growth rates in excess of 30 percent – which the industry saw in both 2016 and 2017. Yet the markedly reduced growth in 2018 gives pause and causes us to question whether the cyber insurance industry can live up to the aggressive growth projections that have been made.[1] One area of encouragement has been in the small commercial cyber, where we estimate that growth and profitability have outperformed the industry overall.

As in prior years, we draw our analysis from US NAIC statutory filings, now in their fourth year of reporting. Although this data set does have limitations and data quality issues, 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.

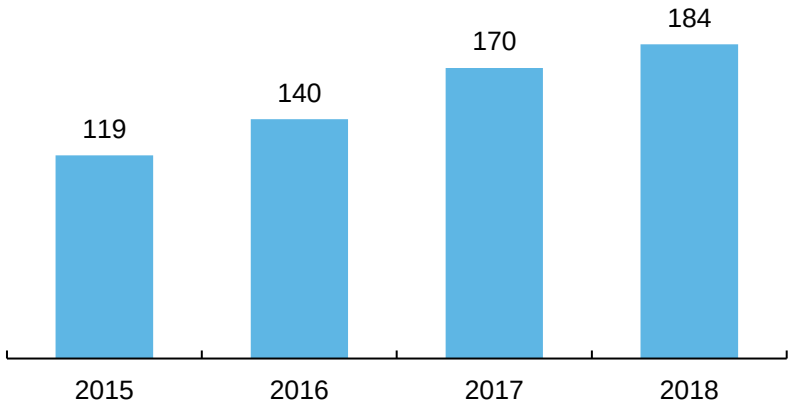
A total of 184 US insurers reported cyber insurance premiums in 2018. Aon has analyzed these filings and shared our key findings on the following pages. Our aim is to provide insights for insurers that currently offer cyber insurance, as well as those seeking to offer it, to provide a performance benchmark, and to give perspective on the industry experience.

Key Findings on 2018 US Cyber Insurance Performance

Premiums and market participation are growing – modestly

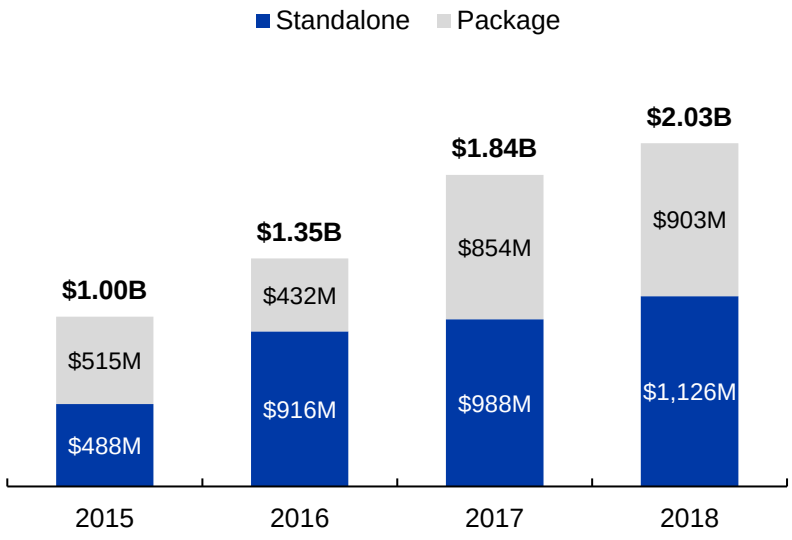
A total of 184 US insurers reported direct cyber written premium to the NAIC in 2018, up from 170 in 2017. The new market participants averaged USD621,000 in premium each. Note that these numbers do not include MGAs.

Exhibit 1: Number of US cyber insurers | 2015 – 2018



US cyber premiums grew to USD2.03 billion in 2018, a 10 percent increase from the prior year. Premiums from package business grew modestly, rising six percent year-on-year. Standalone cyber premiums grew 14 percent. The relative growth rates of package and standalone may be somewhat misleading, however, as several large insurers shifted their reported premium between the categories in 2018.[2]

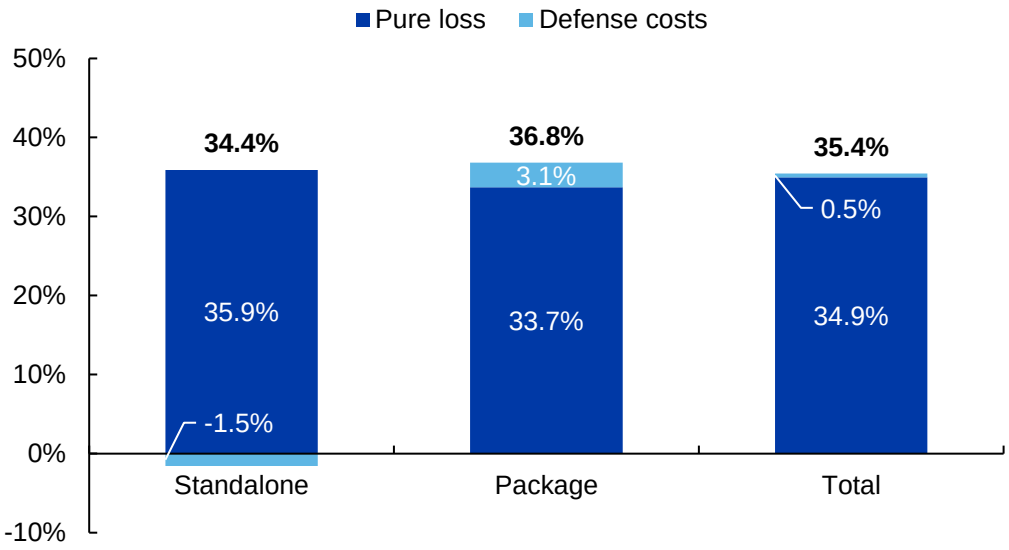
Exhibit 2: US cyber direct written premiums | 2015 – 2018



Loss ratios remained low in 2018, with slight deterioration

The direct incurred industry loss ratio was **35.4** percent across all policies, with standalone and package business reporting 34.4 percent and 36.8 percent respectively. This year, a reporting anomaly resulted in negative average defense costs for standalone insurers, and very low average defense costs for the industry overall.[3]

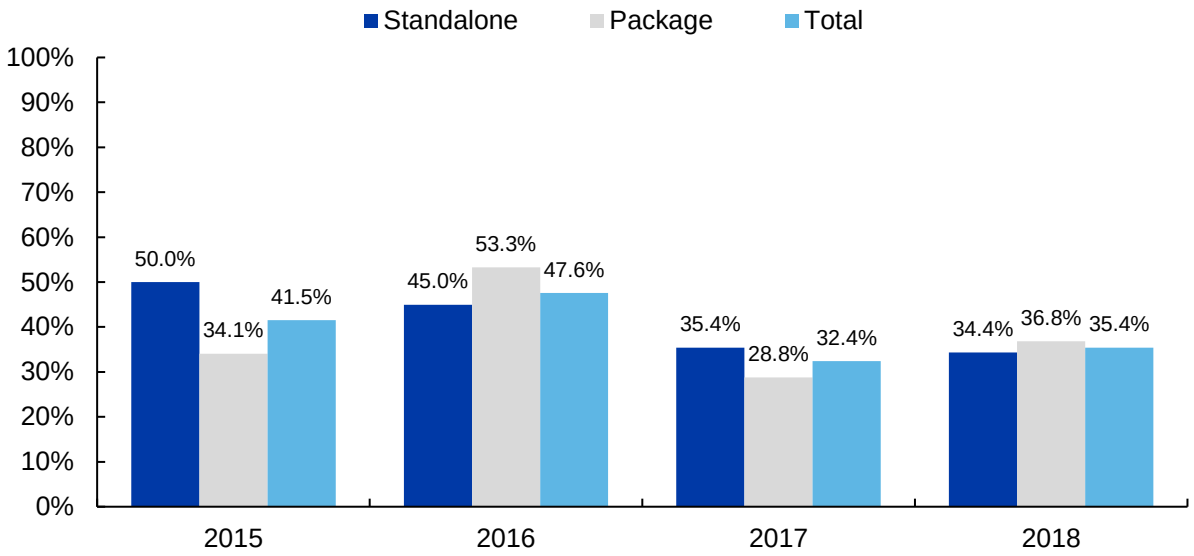
Exhibit 3: US cyber loss ratios | Standalone vs. package



Loss ratios across both the Package and Total segments deteriorated modestly from 2017 but remained lower than 2015-2016 levels. Note that in 2015 and 2016, the NAIC also included adjusting and other expenses in loss ratios, whereas they did not in 2017 and 2018. 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.

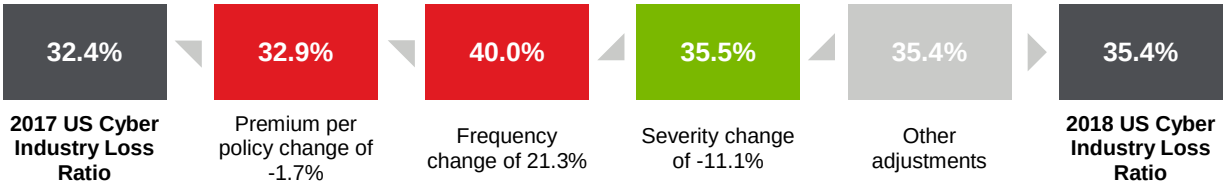
Note that the industry Standalone loss ratio actually improved by 1.0 basis points, to 34.4 percent. The deterioration was on the Package side, where the industry loss ratio rose from 28.8 percent to 36.8 percent in 2018.

Exhibit 4: US cyber loss ratio | 2015 – 2018



We found that the 2018 loss ratio increase was primarily due to an increase in claim frequency. The average 2018 claim frequency across all companies was 4.2 claims per 1000 policies, up from 3.5 in 2017, and affected Package business to a greater degree than Standalone. This jump in frequency more than offset a reduction in the claim severity, where the average claim size fell from USD56,688 in 2017 to USD50,401 in 2018. This shift toward higher frequency and lower severity reflects many of the claims stories of 2018, including increased activity in ransomware, cryptojacking and formjacking claims. Lastly, the premium per policy was slightly down year-over-year, as would be expected in the current soft market conditions.[4]

Exhibit 5: Components of loss ratio change, 2017 to 2018



We also compared loss ratios a different way to see how widespread the year-on-year deterioration appeared to be. Here, we segmented insurers based on the magnitude of their loss ratio change from 2017 to 2018, looking only at writers with at least USD5 million in direct written premium to avoid potential skewing from small premium bases. A change of at least five loss ratio points was selected to indicate a material change. The results appear in Exhibit 6.

Exhibit 6a: US cyber loss ratios, 2017 vs. 2018 | Standalone policies
For insurers with direct written premium greater than USD5 million

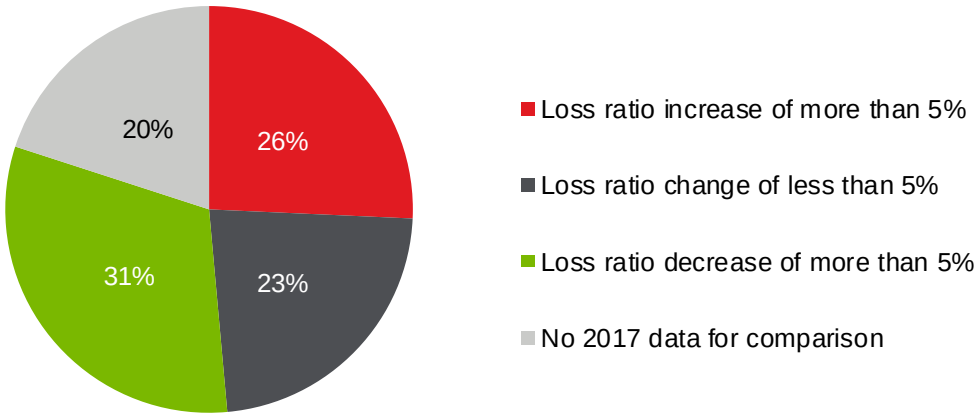
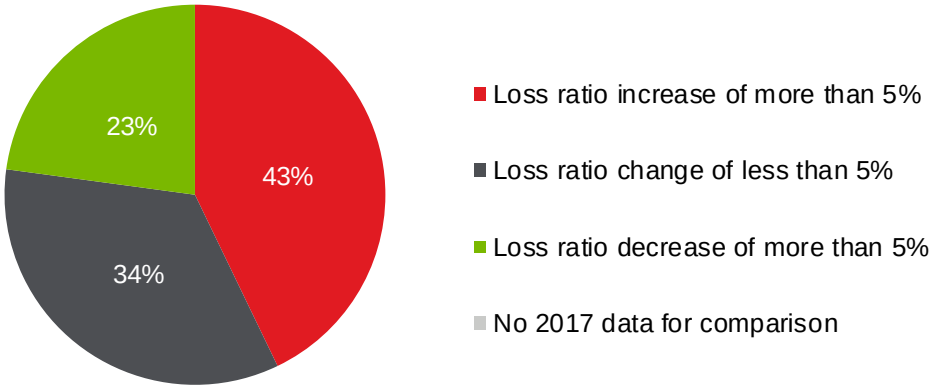


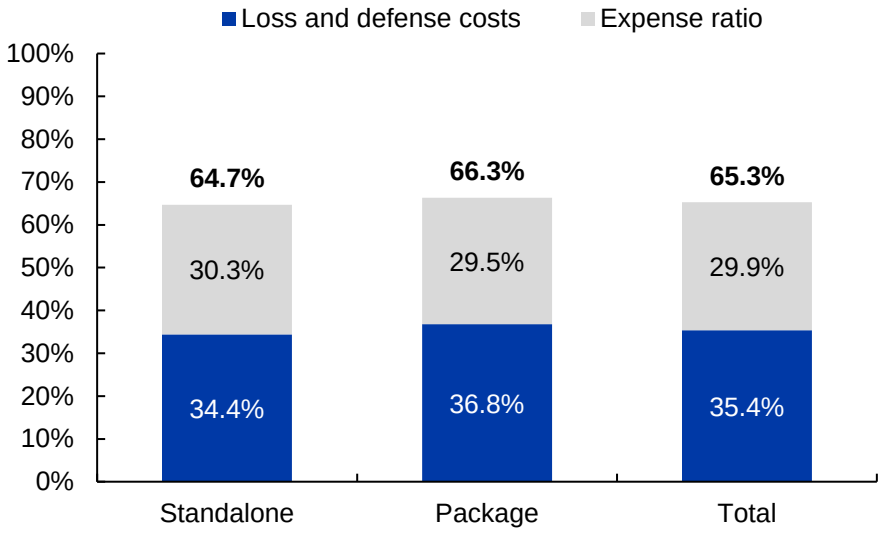
Exhibit 6b: US cyber loss ratios, 2017 vs. 2018 | All policies
For insurers with direct written premium greater than USD5 million[5]



These charts tell a story consistent with the earlier analysis. Overall, more insurers saw increases in loss ratios than decreases in loss ratios when looking at all policies, 43 percent versus 23 percent. When examining just Standalone policies, we saw more decreases than increases, 31 percent versus 26 percent.

Finally, we estimated the industry's cyber combined ratio for 2018, using expense ratio estimates from the Insurance Expense Exhibit.[6] The result appears in Exhibit 7 and further illustrates the profitability of US cyber insurance in 2018.

Exhibit 7: Estimated 2018 US cyber combined ratios



Volatility decreased slightly among insurers in 2018

Individual insurers saw loss ratio results both higher and lower than the average of 35.4 percent – some notably so. Among underwriters with at least USD5 million in direct written premium, loss ratios ranged from 4.8 percent at the low end to 184.4 percent at the high end.

The coefficient of variation (CV) of insurer loss ratios – defined as the standard deviation divided by the mean – decreased modestly in 2018.

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

Calendar Year	Insurers with > USD 5M	Insurers with > USD 50M
2017	116.1%	58.7%
2018	94.2%	50.0%

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 USD5 million in written premium.

Exhibit 9: Cyber insurance loss ratio percentiles by year

Calendar Year	5th Pctl	25th Pctl	Median	75th Pctl	95th Pctl
2017	1.9%	5.4%	25.5%	45.8%	79.3%
2018	5.5%	17.7%	26.4%	53.5%	112.1%

We do see large loss ratios in the data, as seen from the 95th percentile result of 112.1 percent. Also, the median for 2018 is higher than for 2017, 26.4 percent versus 25.5 percent.

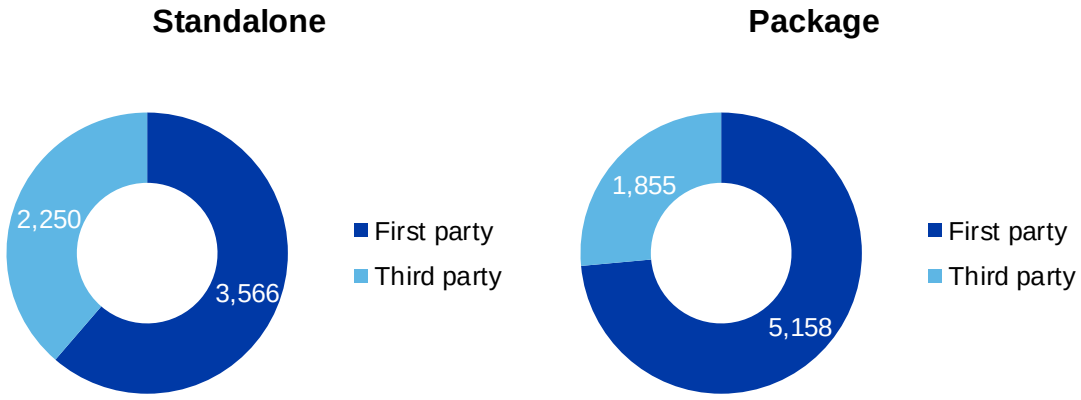
For insurers providing cyber insurance, these results illustrate the potential for both good *and* extremely bad underwriting outcomes and underscore the importance of managing limits.

First party claims predominate

In 2018, claims against first party coverage outnumbered third party claims, accounting for 68 percent of all claims. For standalone policies, first party claims made up 61 percent of the total, while for package policies, first party was 74 percent of the total. The claims results are summarized below.

Exhibit 10: US 2018 cyber claims

Total Claims: 12,829
Total First Party Claims: 8,724 | Total Third Party Claims: 4,105



This is consistent with what we hear from conversations with our clients, with first party claims costs accounting for the majority of costs that insurers are paying.

Claims rates were significantly higher for standalone business. Cyber claims occur at a rate of 46.9 per 1000 standalone policies, versus a rate of 2.4 per 1000 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 slowly, with little new competition

In 2018, US cyber premiums grew approximately 10 percent year-on-year to USD2.03 billion. In total, 184 insurers reported writing some cyber premiums in 2018. This was an increase of 14 insurers over 2017, including 21 new insurers writing premiums that were partially offset by mergers and acquisitions. 88 insurers wrote more than USD1 million and 36 wrote more than USD5 million.

Overall, the market got more concentrated in 2018, not less. The top five cyber insurers accounted for 53 percent of direct written premiums, up from 51 percent last year, and the top 10 accounted for 70 percent versus 69 percent last year. This was a notable change from 2017, where smaller participants grew more rapidly than the market overall.

By way of comparison, the top 10 writers of other liability claims made insurance account for 60 percent of premium and the top 10 in commercial multi-peril account for 47 percent of premium.[7] The US cyber market is still quite concentrated.

The charts below illustrate the distribution of cyber premium.

Exhibit 11: US 2018 cyber direct written premium distribution by insurer size | 2015 – 2018

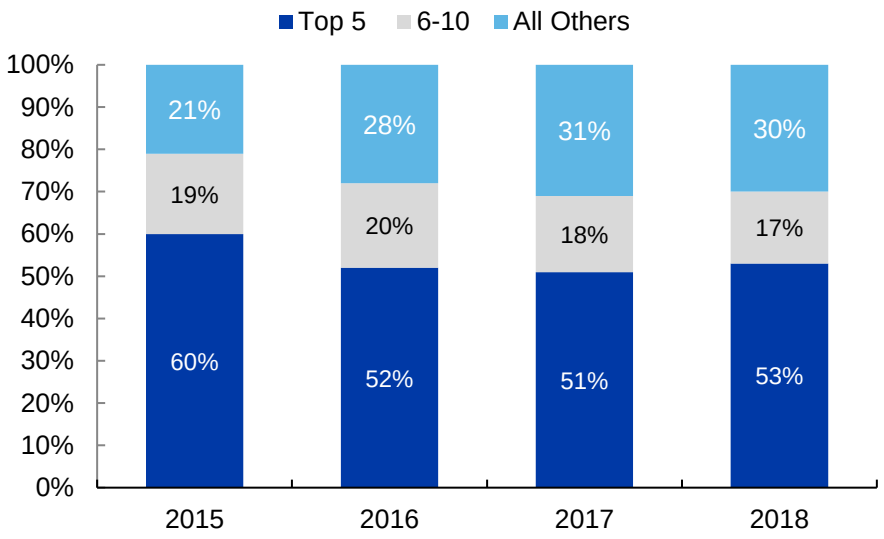


Exhibit 12: US 2018 cyber premium distribution by size rank
Total premium reported: USD2.03 billion

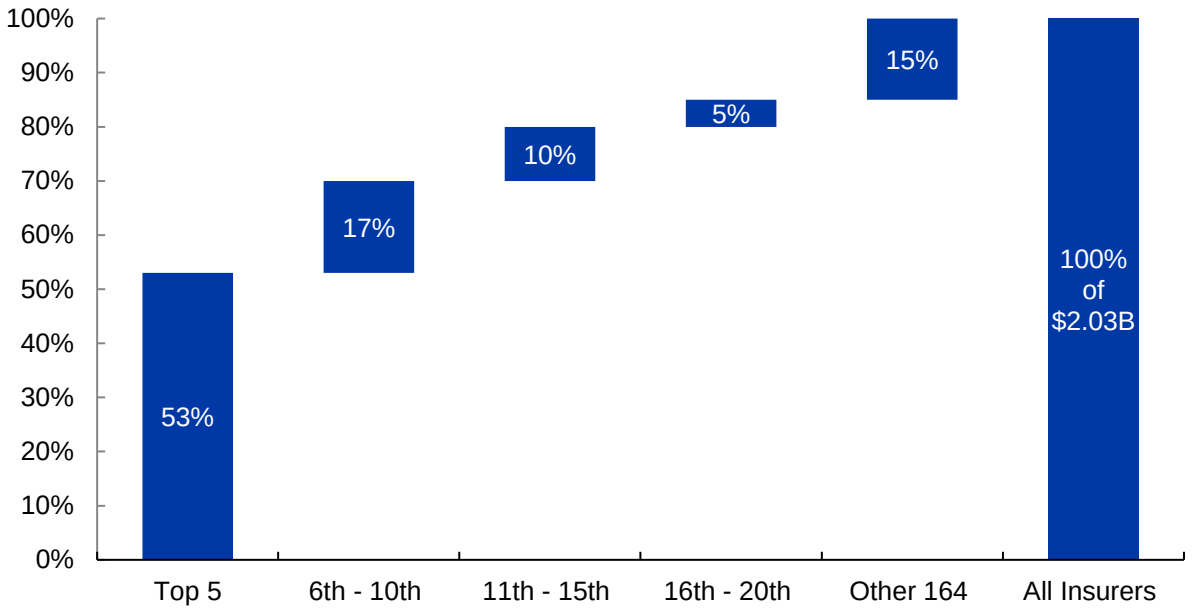
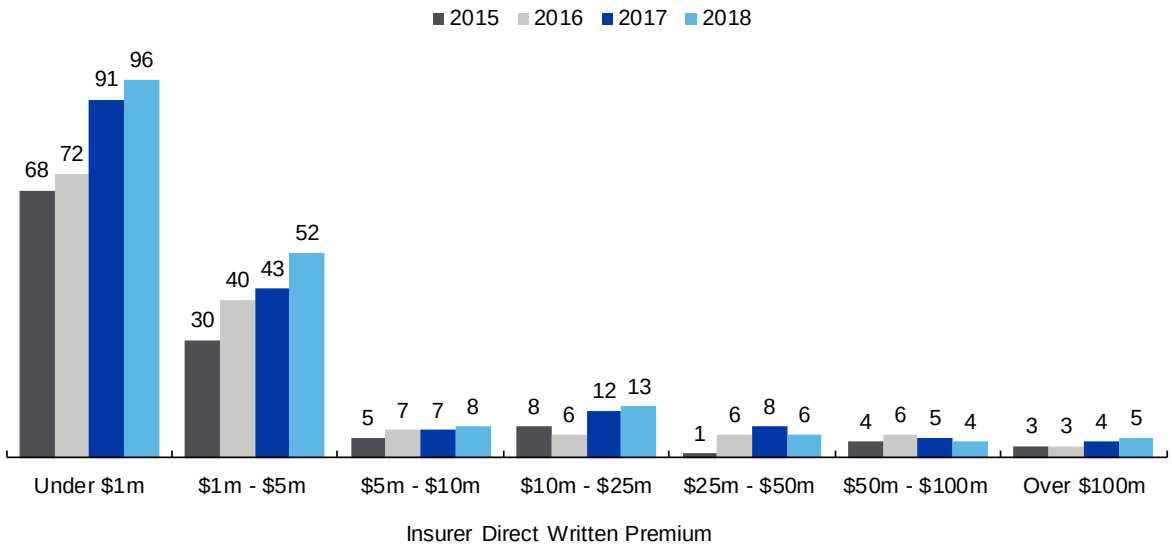


Exhibit 13: Number of US cyber insurers by direct written premium

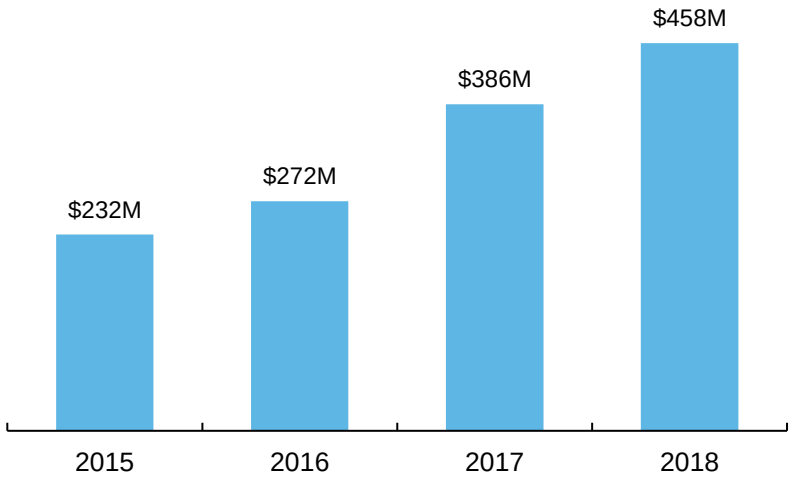


Small commercial cyber is outperforming the industry overall

One relative bright spot in 2018 growth was in the small commercial cyber space. Small and medium enterprise (SME) businesses have been slower to purchase cyber coverage than large corporates, but the growth of this segment is now well underway. SME risks have been highly desirable to insurers given that cyber claims frequency and severity are both lower for smaller companies.[8]

The NAIC data does not neatly allow segmentation by company size. To estimate the SME cyber market, we have focused on the group of insurers that we believe are primarily focused on small commercial accounts and aggregated that group's results. The results can be seen below.

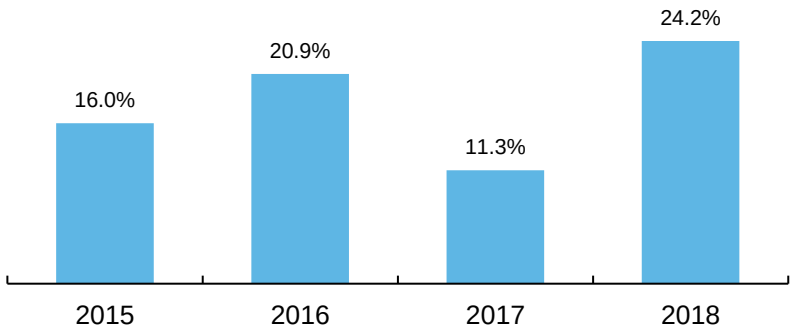
Exhibit 14: US cyber direct written premiums | small commercial writers | 2015 – 2018



Based on this cohort of companies, small commercial cyber premiums grew by nearly 19 percent in 2018 and 42 percent in 2017. The industry overall grew 10 percent and 37 percent, respectively.

Loss ratios in the SME cohort have also performed better than the industry overall, averaging 24.2 percent in 2018.

Exhibit 15: US cyber loss ratio | small commercial writers | 2015 – 2018



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 3, 2019.

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 below.

Premium completeness

The data reported to the NAIC is only a partial picture of the US cyber insurance market. Non-US insurers garner premiums for US risks that are not reflected in this data – most notably, this includes the Lloyd's syndicates. The NAIC data represent a sizable portion of the US market but are not comprehensive. Additionally, the NAIC data do 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 eight percent of the total package cyber premiums reported are from insurers that were unable to quantify the amounts exactly and instead used estimation techniques. However, it's worth noting that this is down from the 23 percent estimated when the NAIC started collecting data in 2015.
- 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 1,000 are collecting more premium. Thus, the results for package business are far less homogeneous than the results for standalone cyber.

Claims data quality

Not all insurers reported cyber claims 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.

Sources and Notes:

[1] Global cyber premium projections have been made of USD14 billion by 2022, and USD20 billion by 2025. These numbers would require sustained annual growth of 20%-26% for the next three to six years, if current global market size is approximated at USD 4.5 billion.

Sources: Allied Market Research, Allianz, Aon research

[2] A number of insurers including Chubb (#1 by total cyber written premium in 2018) and AXIS 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. But for several other insurers including Tokio Marine and W.R. Berkley, we saw the opposite pattern of premiums shifting from package to standalone.

[3] Industry loss ratios are calculated for companies on a calendar year basis and weighted by direct earned premium. All numbers reported to the NAIC are on a direct basis. This year, defense cost ratios were calculated including AIG's reporting of negative Standalone defense costs. This negative value resulted in industry defense cost ratios of -1.5 percent for Standalone and 0.5 percent for the industry Total, respectively. If AIG had been excluded, the defense cost ratios would have been 3.7 percent and 3.4 percent, resulting in total loss ratios of 39.6 percent and 38.3 percent. AIG also reported negative defense costs in its 2017 numbers, but the effect on the industry averages was less pronounced.

[4] Nationwide was removed in the premium per policy and frequency calculations for both 2017 and 2018. Nationwide's 2017 policy count appeared to be an extreme outlier and skewed the calculations. Nationwide's overall loss ratio was quite close to the industry average.

[5] Seven insurers with 2018 premiums had 2017 package premiums but no standalone premiums for comparison. As a result, the standalone chart has 'No 2017 data for comparison' but the total chart does not.

[6] 2018 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).

[7] Source: NAIC 2018 statutory filings, as captured in S&P Global Market Intelligence as of June 3, 2019.

[8] Source: Aon CyberMetrica model research; the relationship between company size (as measured by revenue) and risk has also been corroborated by all the major vendor cyber risk models.

Contact Information

Authors

Jon Laux, FCAS, MAAA
Head of Cyber Analytics
+1 312 381 5370
jonathan.laux@aon.com

Craig Kerman, FCAS
Director, Cyber Practice Group
+1 212 441 1568
craig.kerman@aon.com

Alexa Yakely
Analyst, Cyber Practice Group
+1 212 441 2681
alexa.yakely@aon.com

Aon's Reinsurance Cyber Leadership

Catherine Mulligan
Global Head of Cyber
+1 212 441 1018
catherine.mulligan@aon.com

Luke Foord-Kelcey
Head of Cyber Innovation
+44 (0)20 7086 2067
luke.foord-kelcey@aon.com

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.

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.

Empower Results®