BEST'S MARKET SEGMENT REPORT

June 17, 2019

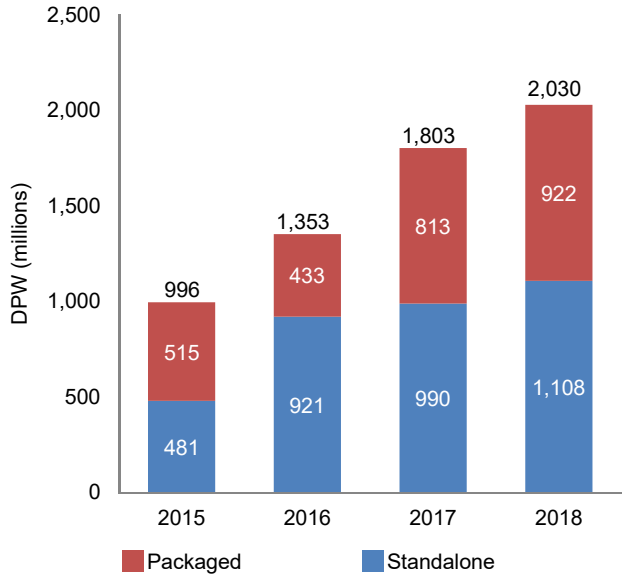
Cyber Insurers Are Profitable Today, but Wary of Tomorrow's Risks

Cyber insurance premiums more than doubled in four years

The market for cyber insurance continued to grow in 2018, according to data from the NAIC's Cybersecurity and Identity Theft Insurance Coverage Supplement (Cyber Supplement). Direct premiums written grew 12.6% for both standalone and packaged policies. Cyber premium volume eclipsed $2 billion for the first time, more than double the amount in 2015. However, growth slowed somewhat from the two prior years, when industry DPW grew more than 30% (**Exhibit 1**). Note that these growth figures may be understated, given that a number of organizations have their own captive insurers to write cyber coverage. Captives have fewer filing requirements and do not file the Cyber Supplement. Without this supplement data, obtaining an accurate measure of the growth of this line isn't possible.

Growth is being driven by organizations wanting to minimize cyber and reputational risk and protect their balance sheets and bottom lines. Additionally, insurers have removed cyber coverage from traditional insurance coverage—by incorporating cyber exclusions in traditional coverages. Growth is also being driven by stricter regulatory environments, led by the General Data Protection Regulation (GDPR) in Europe and similar state-based regulations in the US.

Exhibit 1
US P/C – Cyber DPW



Source: AM Best data and research

Analytical Contacts:
Sam Hanig, Oldwick
+1 (908) 439-2200 Ext. 5520
Samuel.Hanig@ambest.com

Josie Novak, Oldwick
+1 (908) 439-2200 Ext. 5242
Josie.Novak@ambest.com

Fred Eslami, Oldwick
+1 (908) 439-2200 Ext. 5406
Fred.Eslami@ambest.com

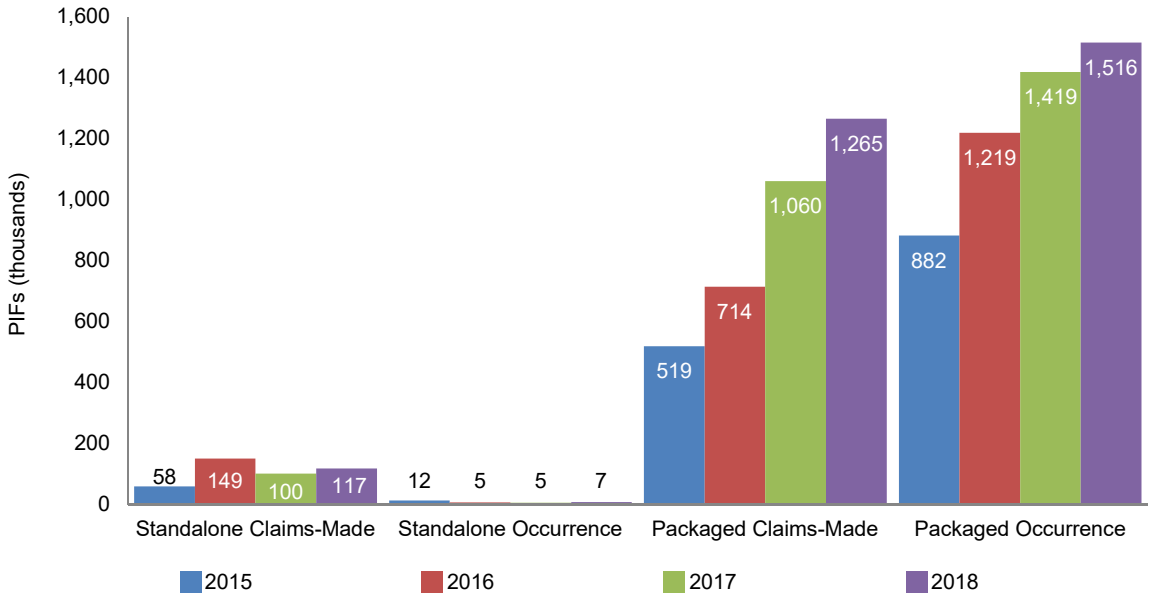
Bob Skrabal, Oldwick
+1 (908) 439-2200 Ext. 5792
Bob.Skrabal@ambest.com

2019-087

NAIC Supplement

The information discussed in this report is based on the Cybersecurity and Identity Theft Insurance Coverage Supplement, which was introduced by the National Association of Insurance Commissioners for year-end 2015. The supplement is broken down based on standalone or packaged coverage. For packaged policies, companies were required to provide either an amount that can be quantified or an estimate for the packaged policies. This information is limited to companies that file annual statutory financial statements with the NAIC; as of this report, 524 insurance companies had done so. Because the supplement was introduced in 2015, AM Best notes that the data quality has certain limitations and that submitted information may not always be accurate or consistent. This does not include non-US or alien surplus lines insurers that do not file the supplement, although we believe that these insurers also write a significant amount of US cyber DPW.

Exhibit 2
US P/C – Cyber Policies in Force by Type



Source: AM Best data and research

Small and medium-sized enterprises (SMEs) are more likely to buy packaged policies (**Exhibit 2**), while larger companies tend to purchase standalone cyber policies with much higher limits. With awareness and demand for cyber coverage growing, many insurers have expanded their product offerings by adding cyber endorsements to their commercial packaged policies (CPP) and business owner's policies (BOP) and packaging cyber coverage with technology E&O policies, which is pressuring other insurers to follow suit, to stay competitive and to meet the demands of policyholders.

The standardization of cyber policy forms has allowed smaller insurers to offer cyber coverage, with many of these carriers ceding 100% of the risk to reinsurers. However, the typical sublimit for cyber coverages on packaged policies offered remains low. A majority of packaged cyber policies tend to be occurrence-based, while standalone policies are generally written on a claims-made basis. However, since the inception of the Cyber Supplement, the percentage of total cyber policies with claims-made triggers has increased. AM Best views this trend positively since claims-made triggers reduce risk and allow insurers to react more quickly to pricing trends, especially for higher limit policies. Companies are also incorporating statutes of limitations in policies to minimize their exposure to first-party claims.

Claims Are Also Growing

First-party claims remain the primary driver of cyber claims, topping 12 million reported claims in 2018 (**Exhibit 3**). Packaged first-party claims breached five million for the first time ever, while total claims exceeded 10 million, another first for the line. First-party coverage applies when the insured (in any industry, offering products and services of any type) is the victim of a cyber incident. First-party coverage includes costs associated with data breach notifications, credit monitoring services for customers, and business interruption resulting from a cyber incident. Third-party coverage is for external businesses or individuals responsible for a cyber event—for example, the vendor of payroll software may purchase third-party coverage, in the event its software is responsible for a breach.

The growth in claims is indicative of a changing market. Claims growth outpaced PIF by 24%: Total claims grew 39%, while total PIF grew 15% (and DPW, 13%)—which AM Best regards as further evidence of growth in SME cyber insurance purchases. Compared to larger companies with larger premiums, smaller companies generally have fewer cyber protections, smaller exposures, lower limits, and commensurate premiums. This lower level of cyber protection makes SMEs more susceptible, which we believe to be the driver of the more rapid increase in total claims. Attritional losses due to ransomware are becoming increasingly common.

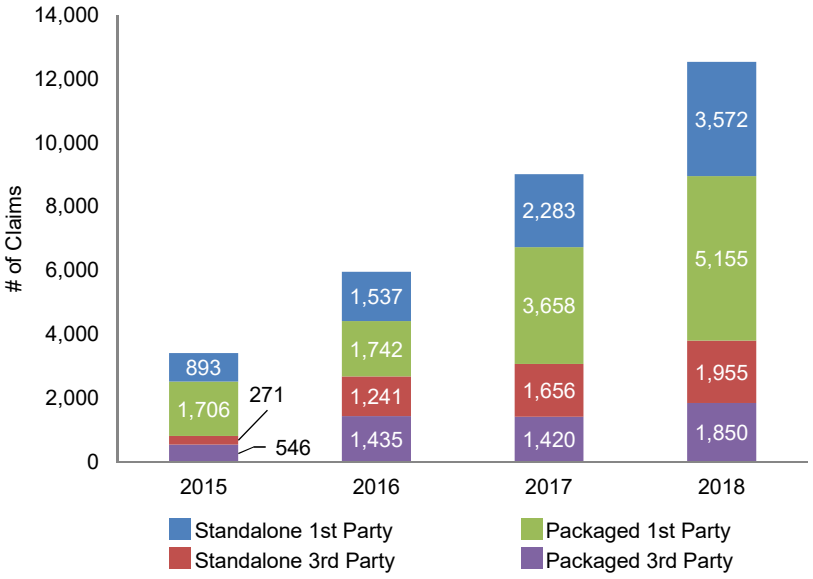
But the Line Remains Profitable

The line's underwriting performance remains strong, with the 2018 direct paid loss & DCC ratios below 25 for both standalone and packaged cyber policies. The packaged paid loss & DCC ratio rose to 24.1 from 13.6, and the standalone's, to 23.2 from 18.8 (**Exhibit 4**). AM Best believes cyber loss ratios are low because, when these policies are priced, carriers apply higher loads owing to uncertainty, compared to other lines. Writers of cyber insurance are still refining their pricing and underwriting. As this line of business stabilizes, more data is gathered, and legal environments become more defined, AM Best expects that the current profitability of cyber insurance will attract more competition, which will ultimately pressure profitability.

A challenge to assessing the profitability of packaged cyber policies is the judgment companies require to allocate a portion of packaged

Exhibit 3

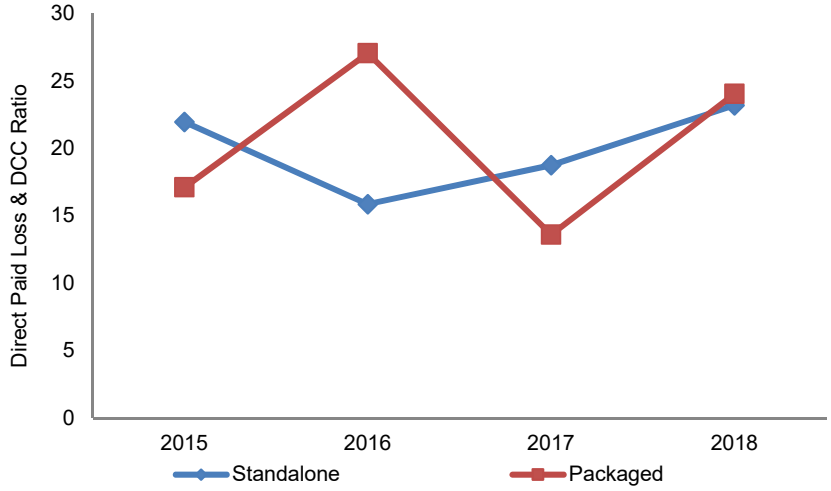
US P/C – Cyber Claims by Policy and Type



Source: AM Best data and research

Exhibit 4

US P/C – Standalone and Packaged Direct Paid Loss & DCC Paid Ratios



Source: AM Best data and research

Exhibit 5
US P/C – Top 20 Cyber Insurers

Rank 2017	Rank 2018	Company Name	2018 DPW ($ millions)	2017-2018 DPW Change (%)	Market Share (%)	% of Cyber DPW Standalone	% of Cyber DPW Packaged
1	1	Chubb INA Grp	325.8	14.5	16.0	1.6	98.4
3	2	AXA US Grp	255.9	43.8	12.6	100.0	0.0
2	3	American International Grp	232.6	1.7	11.4	99.9	0.1
4	4	Travelers Grp	146.2	22.7	7.2	77.2	22.8
6	5	Beazley Insurance Co, Inc.	110.9	16.8	5.5	90.9	9.1
7	6	CNA Insurance Cos	83.4	14.0	4.1	30.0	70.0
5	7	AXIS US Operations	76.0	-25.1	3.7	25.8	74.2
8	8	BCS Insurance Co	69.5	-0.6	3.4	56.9	43.1
9	9	Liberty Mutual Insurance Cos	66.5	10.8	3.3	50.3	49.7
10	10	Zurich Financial Services NA Grp	46.1	7.1	2.3	93.9	6.1
12	11	Allianz of America Cos	46.1	23.6	2.3	24.8	75.2
11	12	Tokio Marine US PC Grp	44.6	11.6	2.2	78.2	21.8
13	13	Hartford Insurance Grp	43.6	25.0	2.1	8.9	91.1
14	14	Sompo Holdings US Grp	40.7	28.3	2.0	16.2	83.8
16	15	Fairfax Financial (USA) Grp	38.2	22.8	1.9	99.8	0.2
22	16	Berkshire Hathaway Insurance Grp	28.6	-0.7	1.4	35.2	64.8
18	17	Markel Corporation Grp	22.5	52.2	1.1	73.5	26.5
21	18	Argo Grp	21.8	2.3	1.1	5.7	94.3
27	19	Aspen US Insurance Grp	21.2	39.2	1.0	99.3	0.7
26	20	The Cincinnati Insurance Cos	16.8	37.7	0.8	0.0	100.0
		Top 5*	**1,071.4**	**17.5**	**52.7**	**66.0**	**34.0**
		Top 10*	**1,412.9**	**12.8**	**69.5**	**61.4**	**38.6**
		Top 20*	**1,737.0**	**12.9**	**85.5**	**58.2**	**41.8**
		Total P/C Industry	**2,032.1**	**12.7**	**100.0**	**54.5**	**45.5**

See shaded text on page 1 of this report.

* Ranked by 2018 total standalone and packaged cybersecurity DPW.

Source: AM Best data and research

policy premiums to cyber. Further, companies may not allocate IBNR reserves specifically to the cyber peril for packaged policies. We expect that, over time, companies will refine these processes for more consistent reporting and to be better able to monitor cyber pricing.

Pricing tends to be driven by supply and demand dynamics, as well as judgment. Although insurers follow systematic questionnaires and checklists, we expect pricing to evolve as insurers gain more experience. Carriers continue to improve their underwriting processes, to be able to write cyber policies in real time. Given that the technology and exposures for cyber change constantly, these underwriting models will never be as precise as those used for property, for example. Some insurers may continue to price a certain risk margin into policies because of the lack of actuarial data and proven cyber exposure models.

Changes in the Top 20 Cyber Insurer Rankings

In 2018, the rankings of the top 20 cyber insurers by DPW saw movement at the top. Chubb moved from second into first place, with $325.8 million in cyber DPW (**Exhibit 5**). AXA, which acquired XL Group in 2018, became the second largest writer, with $255.9 million.

Exhibit 6

US P/C – Top 20 Cyber Insurers by Policies in Force

Rank			PIF* (thousands)		
2017	2018	Company Name	2016	2017	2018
1	1	Hartford Insurance Group	507.5	503.6	510.0
3	2	Liberty Mutual Insurance Cos	158.7	184.5	202.1
2	3	Farmers Insurance Group	147.2	185.8	184.3
6	4	The Cincinnati Insurance Cos	31.6	114.6	179.3
5	5	Berkshire Hathaway Insurance Group	98.1	124.3	146.9
4	6	Erie Insurance Group	124.9	131.6	136.0
7	7	CNA Insurance Cos	63.3	106.9	108.3
9	8	American Family/Main Street America Grp	6.1	79.9	82.8
71	9	Markel Corporation Group	3.1	3.9	68.4
10	10	Selective Insurance Group	54.0	57.5	58.6
8	11	Hanover Insurance Grp Prop & Cas Cos	69.5	94.9	51.7
12	12	Brotherhood Mutual Insurance Co	43.2	48.7	50.4
13	13	West Bend Mutual Insurance Co	25.2	42.2	41.6
20	14	Nationwide Group	27.4	26.5	40.0
18	15	Travelers Group	22.6	29.2	37.0
11	16	W. R. Berkley Insurance Group	53.2	53.4	35.7
16	17	Federated Mutual Group	27.4	31.7	34.4
38	18	Tokio Marine US PC Group	5.5	13.5	33.2
15	19	Doctors Co Insurance Group	0.0	32.0	32.7
41	20	AXIS US Operations	3.7	12.8	29.3
		Top 5	1,036.4	1,129.8	1,222.7
		Top 10	1,319.7	1,583.6	1,676.8
		Top 20	1,585.8	1,936.3	2,062.9
		Total P/C Industry	**2,087.0**	**2,584.1**	**2,905.2**

See shaded text on page 1 of this report.

*Includes standalone and packaged cybersecurity policies.

Source AM Best data and research

AIG, with $232.6 million in DPW, Travelers, with $146.2 million, and Beazley, with $110.9 million, round out the top five. Of the top 20, Chubb, Hartford, Argo, and The Cincinnati Insurance Companies all wrote 90% or more of their DPW as packaged policies, while AXA, AIG, Beazley, Zurich, and Aspen wrote 90% or more of their DPW as standalone policies. The top 10 cyber writers gained market share, increasing to 69.5% in 2018 from 68.2% in 2017, driven by standalone writers claiming more market share. In 2018, the percentages of packaged or standalone policies written changed very little from 2017—a respective 45.5% and 54.5% versus 44.1% and 55.9%. Although the growth in packaged policies was not significant, the SME market still offers potential. Hiscox reports that SME penetration is low, at only 14% (up from 2% in 2014), so the market has ample room to expand. Insurers continue to either add a cyber offering or enhance their existing offering to further tap into the SME market.

At year-end 2018, nearly 3 million cyber insurance policies were in force (**Exhibit 6**), up from 2.6 million the previous year. Hartford remained in the top spot, with just over 500,000 PIF. Liberty Mutual, Farmers Insurance Group, The Cincinnati Insurance Companies, and Berkshire Hathaway Group round out the top five.

Exhibit 7

US P/C – Top 20 Standalone Cyber Insurers' Direct Loss & DCC Ratios

Ranked by 2018 Standalone Cybersecurity DPW

Rank			DPW* ($ millions)		2017-2018 DPW* Change	CY Direct Loss & DCC Ratio*		
2017	2018	Company Name	2017	2018	(%)	2016	2017	2018
2	1	AXA US Grp	177.9	255.9	43.8	65.7	58.4	57.2
1	2	American International Grp	228.7	232.3	1.6	42.4	32.1	36.1
3	3	Travelers Grp	89.1	112.9	26.7	34.3	-5.1	27.7
4	4	Beazley Insurance Co, Inc.	85.6	100.9	17.9	19.8	20.1	6.1
6	5	Zurich Financial Services NA Grp	40.9	43.3	5.9	80.9	67.2	18.2
7	6	BCS Insurance Co	40.3	39.5	-2.0	42.2	39.0	13.5
9	7	Fairfax Financial (USA) Grp	31.0	38.1	23.1	82.5	44.7	23.4
13	8	Tokio Marine US PC Grp	14.4	34.9	142.6	46.9	56.8	38.2
8	9	Liberty Mutual Insurance Cos	32.8	33.4	1.9	87.0	61.9	43.6
10	10	CNA Insurance Cos	23.9	25.0	4.9	7.7	8.8	13.7
12	11	Aspen US Insurance Grp	15.1	21.1	39.2	3.3	5.7	61.6
5	12	AXIS US Operations	45.1	19.6	-56.5	17.2	54.9	1.6
18	13	Markel Corporation Grp	11.9	16.5	39.6	60.0	60.8	60.2
16	14	OneBeacon Insurance Grp	12.2	13.4	10.0	3.0	0.6	53.2
21	15	Allianz of America Cos	9.3	11.4	22.8	0.0	0.0	0.0
19	16	Alleghany Insurance Holdings Grp	11.4	11.1	-2.5	43.9	21.0	12.1
15	17	Hiscox USA Grp	12.6	10.6	-16.1	13.9	13.0	26.8
17	18	Berkshire Hathaway Insurance Grp	12.1	10.1	-16.6	18.2	56.8	82.7
23	19	RLI Grp	5.5	8.8	60.2	17.7	5.1	4.9
20	20	Great American P & C Insurance Grp	9.8	8.6	-12.2	16.5	19.5	36.5
		Top 5	**626.3**	**745.3**	**19.0**	**43.9**	**36.2**	**36.4**
		Top 10	**795.2**	**916.3**	**15.2**	**48.5**	**38.6**	**34.5**
		Top 20	**924.5**	**1,047.6**	**13.3**	**46.0**	**37.0**	**34.6**
		Total P/C Industry	**989.9**	**1,108.4**	**12.0**	**44.1**	**35.4**	**34.3**

* Includes only standalone cybersecurity policies.

Source: AM Best data and research

Smaller insurers are starting to write the line to maintain competitive offerings with carriers already in the market and to meet the rapidly changing needs of policyholders. We expect smaller entities to continue to drive cyber insurance growth, on both buy and sell sides.

By DPW, AXA (owing to the acquisition of XL Group) overtook AIG to become the top standalone cyber insurer, with $255.9 million in cyber DPW, up 43.8% from 2017 (**Exhibit 7**). Although AIG's cyber DPW grew, the growth was minor, only 1.6%, going from $228.7 million to $232.3 million. For 2018, DPW for standalone policies grew 12% versus 8% in 2017. Total DPW for standalone policies was $1.1 billion, up from $989 million in 2017. Standalone performance remained very strong in 2018, with the direct loss & DCC ratio declining for a fourth year, to 34.3 in 2018, down from 35.4 in 2017, 44.1 in 2016, and 64.3 the first year the Cyber Supplement was published. The standalone direct loss & DCC ratio has declined every year since the Cyber Supplement was first filed in 2015.

Exhibit 8

US P/C – Top 20 Packaged Cyber Insurers

Ranked by 2018 Packaged Cybersecurity DPW

Rank			DPW* ($ millions)		2017-2018 DPW Change
2017	2018	Company Name	2017	2018	(%)
1	1	Chubb INA Grp	299.7	320.7	7.0
3	2	CNA Insurance Cos	49.3	58.3	18.4
2	3	AXIS US Operations	56.5	56.4	-0.1
4	4	Hartford Insurance Grp	32.2	39.7	23.3
7	5	Allianz of America Cos	28.0	34.7	23.8
9	6	Sompo Holdings US Grp	27.1	34.1	25.6
5	7	Travelers Grp	30.0	33.3	11.0
8	8	Liberty Mutual Insurance Cos	27.2	33.1	21.5
6	9	BCS Insurance Co	29.6	30.0	1.4
12	10	Argo Grp	18.3	20.6	12.3
13	11	Berkshire Hathaway Insurance Group (G)	16.8	18.6	10.7
15	12	The Cincinnati Insurance Companies (G)	12.2	16.8	37.7
16	13	Hanover Insurance Grp Prop & Cas Cos (G)	11.1	12.8	15.3
14	14	Farmers Insurance Group (G)	13.7	12.6	-7.8
17	15	Beazley Insurance Company, Inc.	9.4	10.1	6.9
10	16	Tokio Marine US PC Group (G)	25.6	9.7	-62.0
21	17	Federated Mutual Group (G)	6.0	8.9	47.3
19	18	Nationwide Group (G)	6.7	7.2	8.6
36	19	Markel Corporation Group (G)	2.9	6.0	103.3
22	20	Constellation Insurance Group (G)	4.7	5.8	22.8
		Top 5	**467.6**	**509.8**	**9.0**
		Top 10	**605.1**	**660.8**	**9.2**
		Top 20	**730.4**	**769.3**	**5.3**
		Total P/C Industry	**813.3**	**921.8**	**13.3**

* Includes only packaged cybersecurity policies.

Source: AM Best data and research

However, these numbers don't reflect the effects of reinsurance, which AM Best believes is heavily used in this market segment. According to Aon, an estimated $800 million in cyber reinsurance was placed in 2018—approximately 40% of all DPW being ceded. Additionally, treaty reinsurance for cyber is now much more widely available than the more expensive and less preferred facultative reinsurance. Most treaties are being written as quota share reinsurance treaties, although most of these agreements include a loss ratio cap.

With plenty of capacity in the property cat market, reinsurers looking to diversify their risk have been actively assuming cyber risk. Aon, for example, launched a $350 million silent cyber facility to protect companies from cyber incidents that could affect multiple lines of business. We would view these participations favorably, so long as the participants are within their well-defined tolerance for cyberevents, have defined risk limits, and use risk modeling to measure the correlated nature of silent and affirmative cyber.

DPW for packaged policies rose 13.3%, to $921.8 million, from $813.3 million in 2017. Some of this growth may be artificial, however, due to a reclassification of premiums. (Companies

Exhibit 9
US P/C – Exposure to Cyber, 2018
Ranked by 2018 Cyber DPW
($ millions)

	2018 DPW			Cyber DPW as a % of	
Company Name	**Cyber**	**Total**	**PHS**	**Total DPW**	**PHS**
Chubb INA Grp	325.8	22,125.3	18,647.1	1.5	1.7
AXA US Grp	255.9	5,256.8	2,511.5	4.9	10.2
American International Grp	232.6	14,815.4	17,909.6	1.6	1.3
Travelers Grp	146.2	26,244.2	20,207.2	0.6	0.7
Beazley Insurance Co, Inc.	110.9	337.1	172.9	32.9	64.2
CNA Insurance Cos	83.4	10,690.9	10,392.5	0.8	0.8
AXIS US Operations	76.0	1,675.3	1,668.8	4.5	4.6
BCS Insurance Co	69.5	367.1	141.9	18.9	49.0
Liberty Mutual Insurance Cos	66.5	34,605.1	19,813.3	0.2	0.3
Zurich Financial Services NA Grp	46.1	12,412.2	6,873.4	0.4	0.7
Total P/C Industry	**2,032.1**	**675,617.3**	**779,163.5**	**0.3**	**0.3**

Includes only companies with $1 million or more in cyber DPW.
Source: AM Best data and research

have reported to AM Best that they are still refining their processes for allocating cyber premiums. As reporting for the supplement becomes more consistent, data collected should become more reliable.) Chubb ($320.7 million) and CNA ($53.8 million) hold the top two spots for packaged cyber insurance (**Exhibit 8**); AXIS, which was third, reported flat growth for packaged cyber DPW in 2018. The top 5, 10, and 20 writers claimed less market share in 2018 than in 2017, as other existing writers, and—to a lesser extent—new packaged writers, garnered more market share.

Concerns and New Risks Continue to Emerge

Cyber risk is unavoidable. According to PwC's Global Cyber Insurance Survey, the biggest challenge for cyber insurers has become managing new risks arising from emerging technologies. The effects of attacks related to emerging technologies include loss of operations, loss of sensitive data, and harm to the quality of an organization's products. With advances in the Internet of Things and Big Data, there are more cyber access points susceptible to breaches providing access to ever increasing volumes of private company data.

Cyber business interruption/continual business interruption is difficult to underwrite, even as demand for this coverage grows. Most companies writing cyber insurance are remaining prudent about their total exposure, and cyber exposure relative to policyholder surplus is limited. Of the top 10 cyber insurers, Beazley and BCS have the highest cyber DPW relative to surplus, with the rest of the top 10 having minimal exposure (**Exhibit 9**). However, these figures do not include assumed or ceded reinsurance or exposure to silent cyber, so the actual net exposure may be larger or smaller.

Although underpricing by new market entrants is an industry concern, a systemic event remains the top threat to cyber insurers' solvency. A systemic event has the potential to cause extensive losses, although these may be mitigated somewhat by infrastructure exclusions.

We are also seeing new types of cyber exposures emerging, in the form of Meltdown and Spectre, which target hardware vulnerabilities in processors (not just in computers and

phones, but even data stored in the cloud)—not specific software. Developers have created patches to address these threats, but these are atypical risks that all companies are exposed to.

Recent Notable Cyber Incidents

In November 2018, Marriott International announced that a breach of its Starwood Guest Reservation database had exposed up to 383 million guest records (including passport numbers, names, addresses, dates of birth, emails, and more) going back to 2014. Although payment card numbers were encrypted, parts of payment card numbers could have been entered into unencrypted fields or decrypted. As recompense, Marriott offered free Webwatcher enrollment—software that monitors internet sites where personal information is shared and generates a consumer alert if evidence of the consumer's personal information is found—for a year to all victims of the breach, as well as a dedicated website and call center so victims could monitor and protect their information.

Also in 2018, Wired Magazine broke the story of unsecured records at marketing firm Exactis, which affected 340 million records. The data included both personally identifiable and business information, but did not appear to leak payment card or social security numbers. Whether criminals or hackers accessed the database was unclear, but (per the person who discovered the breach) the data would have been easy to find for a hacker with even basic experience.

Additionally, 2018 confirmed that even titans of the technology industry remain exposed to cyber risk. In October, Google announced that it was shutting down its Google+ social network following the discovery of a bug in a software update that exposed the personal data of more than 52 million users. And, in December, Facebook announced that up to 30 million people had been affected by a hack where access tokens were stolen, including personally identifiable information, customers' recent searches, the devices they used to log into Facebook, and other sensitive data.

Midway through 2019, it was reported that more than 800 million lending documents (dating back to 2003) of First American Financial Corp, a real estate title insurance company, had been unprotected. These unsecured documents included personal information like bank account numbers, driver's license images, social security numbers, tax receipts, and more. The data was accessible on the company's website. On May 31, 2019, AM Best commented that the Financial Strength Rating of A (Excellent) and the Long-Term Issuer Credit Ratings (Long-Term ICR) of "a" of the members of First American Title Insurance Group, as well as the Long-Term ICR of "bbb" of the parent holding company, First American Financial Corporation (First American) (Delaware) [NYSE: FAF], remain unchanged following the organization's announcement that investigations into a reported information security incident are ongoing.

What gets lost in the publicity of these high profile cyber exposure events is that there is little, if any, publicity for smaller companies experiencing a cyberattack. SMEs are actually at greater risk, as they are easier targets because of generally weaker cybersecurity. According to a 2018 mid-year survey by Argo Group, only 40% of SMEs purchase some form of cyber insurance.

Cyberattacks: Acts of War … or Not

Following the NotPetya attack in 2017, which targeted companies such as Maersk, Merck, and FedEx, Mondelez International was also severely hampered by the malware. The company incurred more than $100 million in losses and sought indemnification from its cyber insurer, Zurich. The legal issues rest on whether the attack could be construed as an act of war. The cyber community is watching developments as they play out in the courts, as the results could have an impact on underwriting and policy language and insurance purchases.

Risk managers and brokers must consider what clarity and assurances they can obtain to minimize the risk that insurance companies will attempt to deny coverage due to the war exclusion. Companies should be looking carefully at the "act of war" exclusionary language and negotiate changes. AM Best will continue to monitor how these legal battles play out in the courts.

The US Treasury published guidance in 2013 that states that a cyberattack could be considered an act of terrorism and that standalone cyber liability is subject to TRIPRA (the Terrorism Risk Insurance Program Reauthorization Act). As TRIPRA expires on December 31, 2020, AM Best will evaluate insurers' contingency plans for the potential loss of the federal backstop.

Regulatory Schemes Still Evolving

Regulations specifically regarding data breaches are expanding, with the strictest laws so far coming from New York State (NYCRR 500) and Europe under the GDPR. These laws and regulations are designed to ensure that companies and organizations do all they can to protect their systems and data from viruses, Trojan horses, phishing, and distributed denial of services (DoS) attacks, as well as unauthorized access that leads to the stealing of intellectual property or confidential information.

Risk stemming from regulatory changes has grown significantly in recent years owing to the increase in cyber breaches as well as hackers' growing sophistication. The burgeoning attention to regulatory issues reflects the proliferating responsibility regulators are placing on companies. Companies in some jurisdictions are now required to notify their customers of data breaches instead of just trying to sweep them under the rug. Unlike Europe, the US has yet to create an overarching federal cybersecurity law. However, the absence of a federal regulation has not precluded the states from addressing the issue.

Individual states are addressing these concerns through initiatives such as providing more funding to improve security measures or requiring entities to implement specific types of security practices. In 2018, at least 22 states, in addition to Washington, DC, and Puerto Rico, introduced more than 52 cybersecurity-related bills or resolutions. The key areas of legislative activity include improving government security practices or promoting workplace training. Some states have particularly strict cybersecurity laws, but details for when a company is fined for noncompliance are scarce. Companies that operate in multiple states—online companies, for example—are subject to the cybersecurity laws in all of those states as well.

The most notable regulation passed in 2018 was the California Consumer Privacy Act, set to take effect in 2020. This regulation applies to California residents' personally identifiable information, in effect a Bill of Rights covering consumers' information, and mandates stricter security and privacy requirements for California-based companies, which will be subject to large fines and penalties for non-compliance.

Additionally, in 2018, the US Securities and Exchange Commission become involved in cyber regulation, requiring cybersecurity disclosures in a company's financial statements. The SEC also issued its first fines for cybersecurity, which shows how cyber regulation enforcement is becoming more aggressive.

Regulations in Europe

The regulatory landscape in Europe changed markedly, with the May 2018 passage of the GDPR. Companies that collect personally identifiable information in Europe now have to deal with

potentially sizable financial and reputational consequences under the GDPR. This regulation radically changes how EU constituents approach data privacy and the protection of EU citizens' personal data. GDPR requirements apply to each of the EU's member states and aim to create a more consistent approach to protect consumer and personal data in all EU nations. It is not only a European concern, as the GDPR requirements apply to all companies operating in the EU, regardless of where they are domiciled or where the data processing takes place.

GDPR gives ownership and control of data usage back to customers—meaning that a large company that captures consumer data can no longer claim this data as its own asset. Organizations may not transfer any data to a third party without the consumer's express approval. Consumers are particularly concerned about a potential loss of privacy, given the explosion in social media usage, as well as the accompanying growth in high-profile data breaches and incidences of fraud. These concerns led to some of the GDPR's key privacy and data protection requirements, which include requiring the consent of consumers for data processing and safe handling of the transfer of data across borders, as well as the appointment of a data protection officer at certain companies to oversee compliance with GDPR. Entities must also report a breach within 72 hours of detection. If an organization fails to comply with the regulations, it is liable for fines of up to 20 million euros (USD 22.3 million) or 4% of global annual turnover—whichever is higher.

The UK has implemented its own requirements. The UK's Prudential Regulation Authority Supervisory Statement SS4/17 outlines new requirements for insurers to manage their cyber risk. It mandates that firms be able to identify, quantify, and manage cyber insurance underwriting risk from both affirmative cyber risk in policies explicitly covering cyber risk and non-affirmative (silent) cyber risk included in other property/casualty policies. The statement also outlines expectations for how Solvency II firms assess and manage their cyber exposures.

The Path Forward

In 2018, 528 US insurers reported writing cyber insurance, up from 471 in 2017, 400 in 2016, and 309 in 2015. According to a survey by Argo Group, 73% of brokers reported that the most common security problem clients face is phishing. Employees may not act maliciously, but may make a mistake unintentionally—for example, opening an email that looks as if it came from a company executive or a legitimate company, that actually contains a virus designed to infiltrate the company's database. Companies are vulnerable to hacks though their employees' work computers or laptops, or through the loss of a computer with unencrypted company information.

Furthermore, corporations are not the only entities at risk. The last few years have seen a marked increase in ransomware attacks on municipalities, including Atlanta and Baltimore, with legacy and old systems, a trend that will only continue to grow.

Cyber risk modeling is in its infancy, as events and threat vectors are still evolving. To simulate the event sets and fit them into traditional statistical distributional forms is the first challenge. Cataloging the exposure in an insurer's portfolio to these events and how the losses vary depending on the severity of the attack and estimating the financial damage are all complicated problems that cyber modeling firms are tackling. These models are improving and may provide directional input into relative rankings of risk but need to be complemented with stress testing and analytical, experience-based judgment for pricing, capital consumption, and allocation.

We believe the cyber insurance market presents a positive opportunity for insurers. As companies' exposures to cyber risk continue to grow, so too will the demand for cyber

insurance. Capacity should also continue grow, given that the line's profitability will undoubtedly attract more new market entrants. A lot of cyber risk is embedded, but standalone cyber premium should continue to grow as companies add exclusions to other policies, and coverage for cyber policies broadens. While the cyber insurance market grows, AM Best will continue to monitor how insurers are managing their own cyber insurance exposure, and that these exposures are sufficiently taken into account in their own enterprise risk management processes. Insurers will continue to offer cyber for diversification with reinsurance support and careful limit structures. Cyber insurance growth without corresponding risk controls would be deemed credit negative.

Published by AM Best

MARKET SEGMENT REPORT

A.M. Best Company, Inc.
Oldwick, NJ
CHAIRMAN, CEO & PRESIDENT **Arthur Snyder III**
SENIOR VICE PRESIDENTS **Alessandra L. Czarnecki, Thomas J. Plummer**

A.M. Best Rating Services, Inc.
Oldwick, NJ
CHAIRMAN, CEO & PRESIDENT **Larry G. Mayewski**
EXECUTIVE VICE PRESIDENT **Matthew C. Mosher**
SENIOR MANAGING DIRECTORS **Douglas A. Collett, Edward H. Easop, James Gillard, Stefan W. Holzberger, Andrea Keenan, James F. Snee**

WORLD HEADQUARTERS
1 Ambest Road, Oldwick, NJ 08858
Phone: +1 908 439 2200

APAC REGION – HONG KONG OFFICE
Unit 4004 Central Plaza, 18 Harbour Road, Wanchai, Hong Kong
Phone: +852 2827 3400

APAC REGION – SINGAPORE OFFICE
6 Battery Road, #39-04, Singapore
Phone: +65 6303 5000

EMEA REGION – AMSTERDAM OFFICE
NoMA House, Gustav Mahlerlaan 1212
1081 LA Amsterdam, Netherlands
Phone: +31 20 308 5420

EMEA REGION – LONDON OFFICE
12 Arthur Street, 6th Floor, London, UK EC4R 9AB
Phone: +44 20 7626 6264

LATAM REGION – MEXICO CITY OFFICE
Paseo de la Reforma 412, Piso 23, Mexico City, Mexico
Phone: +52 55 1102 2720

MENA REGION – DUBAI OFFICE*
Office 102, Tower 2, Currency House, DIFC
P.O. Box 506617, Dubai, UAE
Phone: +971 4375 2780
*Regulated by the DFSA as a Representative Office

Version 020419