MOODY'S
INVESTORS SERVICE

SECTOR IN-DEPTH
25 July 2019

Rate this Research

Contacts

Sarah Hibler +1.212.553.4912
Associate Managing Director
sarah.hibler@moodys.com

Marc R. Pinto, CFA +1.212.553.4352
MD-Financial Institutions
marc.pinto@moodys.com

Simon Harris +44.20.7772.1576
MD-Gbl Ins, Fnds & Asset Mgmt
simon.harris@moodys.com

» Contacts continued on last page

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

P&C Insurance — Global

Battling hidden cyber exposures, insurers position for growing opportunity

While property and casualty (P&C) insurers are at risk of cyberattacks themselves, they are also in the unique position of providing other companies insurance coverage for attacks. However, not all cyber coverage takes the form of cyber insurance, a separate product type. Some cyber coverage is "silently" embedded in commercial property and liability policies because of ambiguous wording or because it is not excluded from those policies. Consequently, accurate assessment and management of cyber exposure is a top priority for P&C insurers, especially since commercial property policy limits are often multiples of limits provided for cyber-only coverage. We continue to view cyber insurance as a high-risk product, but insurers have generally taken a measured approach with the support of reinsurance.

» **A small but profitable line for most insurers with increasing demand for coverage.** Cyber insurance, although still a small market, has grown quickly in the four years since our initial report on the product. It is a highly profitable business for those insurers that continue to invest in underwriting, modeling and analytics. Growth prospects for cyber insurance are promising given the changing nature of the risk, the pervasiveness of technology, the value of insurance as a risk management tool, and expanding regulation, all of which are driving demand for coverage.

» **Assessing aggregate insured cyber exposure is complicated.** In addition to embedded cyber exposures in traditional P&C policies, ongoing cyber-related insurance litigation complicates true cyber exposure assessment. Two closely watched court cases will determine whether certain exclusions found in most traditional P&C policies can apply to cyberattacks. Other ongoing litigation addresses who has a legal basis to sue for damages in cyberattacks that result in stolen personal information.

» **Underwriting and risk management projects begin to address silent cyber exposures.** Insurers, particularly those that write large national and multinational accounts, are shifting cyber risk to standalone policies or implementing cyber sub-limits or exclusions in traditional policies. Insurers and reinsurers are also using deterministic scenarios and working with third party vendors to model cyber risk.

» **Unique difficulties remain for underwriting cyber insurance.** A lack of uniform policy wording and the evolving nature of the risk constrain the growth of cyber insurance as a separate product. Potential risk accumulations are another challenge because the same event can affect multiple clients, particularly as companies move to cloud computing.

A small but profitable line for insurers with increasing demand for coverage

Insurers' revenue from cyber insurance has increased rapidly in recent years, along with demand from private and public enterprises. The intensification of cyberattacks and the associated costs, the heightened focus by boards of directors and risk managers, as well as recent regulations are driving demand and the increasing number of insurers offering cyber insurance.

Based on US regulatory financial data, direct cyber premiums written grew to $2 billion in 2018, or a cumulative annual growth rate of 26% since 2015. Despite the fast growth, cyber insurance still comprises less than 1% of US industrywide premium revenue, which is dominated by personal automobile and homeowners' insurance as well as standard and specialty commercial insurance.

More than 40 US insurance groups underwrite cyber insurance as standalone coverage, but the market remains concentrated among the largest commercial insurers, with the top two (Chubb Limited and AXA SA) accounting for nearly 30% of the US market. The Top 10 cyber insurance carriers collectively account for more than two thirds of the market (see Exhibit 1). For most of these insurers, cyber premiums contribute less than 2% of US direct premiums written. Top writers of global cyber insurance include Chubb, AIG, Allianz, AXA, Zurich and several Lloyd's syndicates.

Exhibit 1

Leading US underwriters of cyber insurance in 2018

$ Millions

	Company Name	Senior Debt Rating	US Cyber DPW	US Cyber Market Share	US All Lines DPW	US Cyber % All Lines
1	Chubb	A3 / Pos	$326	16.3%	$22,009	1.5%
2	AXA	A2 / Sta	$256	12.8%	$5,257	4.9%
3	AIG	Baa1 / Sta	$233	11.6%	$14,725	1.6%
4	Travelers	A2 / Sta	$146	7.3%	$26,244	0.6%
5	Beazley Insurance Co.	NR	$111	5.5%	$337	32.9%
6	CNA	Baa2 / Sta	$83	4.2%	$10,691	0.8%
7	AXIS	Baa1 / Neg	$76	3.8%	$1,675	4.5%
8	BCS	NR	$70	3.5%	$367	18.9%
9	Liberty Mutual	Baa2 / Sta	$66	3.3%	$34,605	0.2%
10	Zurich	A1 / Sta	$46	2.3%	$12,412	0.4%
	Top 10		**$1,413**	**70.5%**	**$128,322**	**1.1%**
	Total US P/C Industry		**$2,004**	**100.0%**	**$671,918**	**0.3%**

BCS Insurance Company provides cyber and privacy loss protection policies to Blue Cross Blue Shield companies; Beazley Insurance Company is part of Beazley PLC.
Source: SNL Financial LC. Contains copyrighted and trade secret materials distributed under license from SNL, for recipients' internal use only

Increasing claims, including for data breaches, denial-of-service attacks and the financial demands of ransomware attacks are spurring demand for cyber insurance in a number of industries. Some cyberattacks have been widely publicized, but they are vastly outnumbered by lower profile or unpublicized incidents. According to the nonprofit organization Identity Theft Resource Center (ITRC), although the number of breaches in 2018 reported publicly declined by 23% to 1,244, the total number of personal records exposed by cybersecurity breaches rose by 126% to 446.5 million, with the Marriott International breach in 2018 having the largest number of records exposed.

Cyberattack remediation can be costly, resulting in business interruption and reputational damage, and can lead to litigation by shareholders and other injured parties. Also, costs remain overwhelmingly concentrated in advanced economies. In its 2019 Cost of Cybercrime Study, [1], the Ponemon Institute, sponsored by Accenture Security, said that for US companies participating in its research, the average cost of a cyber crime was about $27 million in 2018 – the highest total average cost of the 11 countries in the study – up 29% from $21 million in 2017.

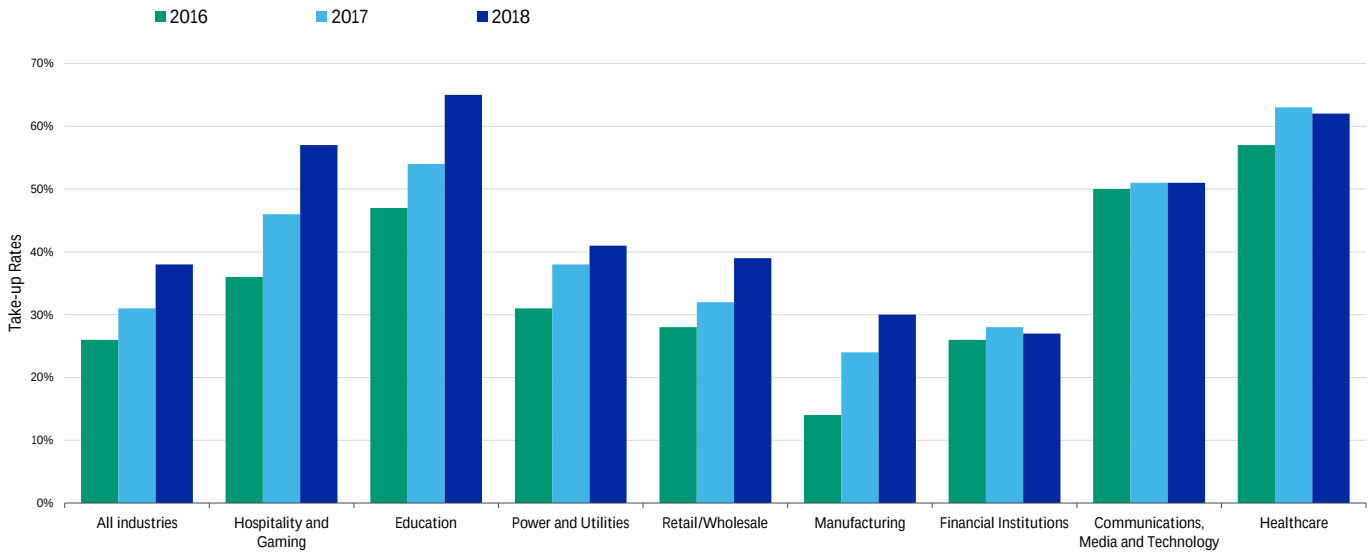
The largest institutions with the most formalized governance structures are the dominant buyers of cyber insurance protection. Not only have a growing number of large firms purchased cyber insurance, they have also increased the limits of protection they purchase, with program limits of $25-$100 million now common, compared with norms of $10-$15 million just a few years ago. Presently, more firms can purchase as much as $750 million in limits, with insurance brokers continuing to build higher-limit cyber insurance programs.

Cyber insurance coverage has expanded over the past several years to include not just data breaches, but also cyber extortion, social engineering, corporate identity theft, contingent business interruption, reputation loss, and other effects depending on the specific policy wordings. One of the important benefits of cyber insurance coverage is post-attack remediation services.

Smaller enterprises in a number of industries generally have lower penetration or take-up rates of cyber insurance than larger institutions. In lieu of standalone or packaged coverage, these smaller firms have purchased "cyber-lite" protection, which offers insurance similar to larger coverage but which has smaller sub-limits and is not individually underwritten. Among middle-market and larger firms in a number of industries, penetration of cyber insurance has increased notably because these firms have more coverage options available to them than in the past. Take-up rates by these institutions have broadly increased in lockstep over the past few years (see Exhibit 2), reflecting increased risk awareness, broad-based market acceptance of cyber insurance products, as well as demands by supply-chain counterparties.

Exhibit 2

Take-up rates for cyber insurance by industry sector



Source: Marsh Data, Analytics and Digital, PlaceMAP

Regulators across the globe have raised the bar for protection of consumer and personal information. More than 100 countries have implemented or are in the process of passing some form of data privacy and protection legislation. In addition to US privacy regulations, in the EU the most notable regulation was the General Data Protection Regulation that went into effect in May 2018. The proliferation of new rules around the globe has boosted demand for cyber insurance, but has also raised questions and uncertainty around the scope of the insurance coverage.

For example, cyber insurance policies generally cover losses related to data breaches, but it remains unclear whether they will be able to cover losses related to fines. In most jurisdictions, insurers are legally prohibited from indemnifying fines and regulatory penalties since doing so may undermine the intention of the law, which is to assure compliance rather than to treat noncompliance as a cost of doing business.

As a result of increasing regulations, particularly the General Data Protection Regulation, we expect that cyber insurance premiums will gradually increase in Europe. Some Asian insurers in countries like Japan are starting to develop cyber insurance products. Insurers continue to monitor global legislation and update their cyber coverage and pricing models accordingly.

Recent regulation boosts US and international demand for cyber insurance

California Consumer Privacy Act (CCPA). California signed CCPA into law in June 2018 and it takes effect July 1, 2020. CCPA is designed to enhance the privacy rights and consumer protection for California residents. The law applies to any business that collects consumers' personal data and does business in California. The California attorney general can impose fines for data violations up to $2,500 per violation if not cured within 30 days. According to law firm Skadden, Arps, Slate, Meagher & Flom, CCPA makes it easier for consumers to sustain a data breach claim because it does not require a show of harm from the incident. In different jurisdictions, many data breach cases are dismissed for lack of standing.

General Data Protection Regulation (GDPR). According to the GDPR, any organization that holds data on European Union citizens, regardless of where the data is stored or domiciled, must follow this comprehensive data protection law. The principles-based regulation, which took effect in May 2018, compels organizations to implement controls that are commensurate with their risk. Regulators are able to impose fines that can range up to the higher of €20 million or 4% of a company's global annual turnover.

New York State Department of Financial Services (NYDFS) cybersecurity regulation. Effective March 1, 2017, the New York State Superintendent of Financial Services established cybersecurity requirements for financial services companies. Among other items, the regulation requires a cybersecurity plan, the designation of a chief information security officer, and the maintenance of an ongoing reporting system for cybersecurity events. The last phase of the regulation, effective March 1, 2019, requires companies to have policies in place to manage cyber risk associated with all third-party vendors and suppliers.

National Association of Insurance Commissioners (NAIC) data security model law. The NAIC created a data security model law in 2017, which is similar to the NYDFS cybersecurity regulation, and which the US Treasury Department endorsed. South Carolina in 2017 became the first state to adopt it, and more recently, Ohio and Michigan have adopted it. Other states will likely adopt the law over the next few years, with some states enacting it as is and others modifying some of the components.

Biometric Information Privacy Act (BIPA). In 2008, this Illinois law required companies doing business in the state to obtain written consent from an individual before collecting biometric identifiers. Since biometric data cannot be changed – unlike a credit card number, for example – theft of this data presents a higher risk to companies and their insurers than other forms of data theft. Companies must also disclose their policies regarding the use and retention of biometric data. Currently, Illinois law allows private suits and recovery of damages for violations ($1,000 fine per infraction, and $5,000 per infraction if a company is found to be intentionally violating the act). Other states, such as Washington and Texas, have passed similar legislation and more are considering doing so.

Assessing aggregate insured cyber exposure is complicated

In our February 2019 cyber risk report, we assess 11 sectors including P&C insurance companies as having medium risk. P&C insurers provide cyber insurance coverage to other companies for cyberattacks while also risking such attacks themselves. However, not all cyber coverage takes the form of cyber insurance, a separate product type. Accurately assessing and managing cyber exposure is a top priority for P&C companies, especially following the 2017 NotPetya malware attack against Ukraine that caused severe damage to corporations across the globe and involved dozens of insurers and reinsurers.

A number of complex claim and coverage issues in the past several years have led to significant uncertainty in the marketplace for both insureds and insurers, such as whether cyber insurance responds to physical damage claims for property, including business interruption and contingent business interruption losses. Commercial property exposure limits are often multiples of limits for cyber-only coverage, which dramatically raises the stakes for losses and risk aggregation and highlights the challenge for assessments.

In addition, the potential for exposure accumulations from the same loss affecting multiple insured clients as businesses move to cloud computing and the longer-term threats posed by quantum computing all complicate exposure management.

Cyber risk is embedded in traditional P&C policies because of ambiguous wording or not being explicitly excluded

A single cyber event can swiftly and severely affect multiple sectors, companies, supply chains, logistics and production capacity. The NotPetya attack had effects far beyond its intended target of state and private-sector organizations in Ukraine, showing the

disruptive potential of a severe cyberattack. NotPetya as well as other attacks highlighted an issue that P&C insurers and reinsurers had discussed for several years: silent or non-affirmative cyber risk. Silent cyber refers to traditional P&C policies such as property and general liability that were not originally intended to provide cyber protection, but because policy wording was ambiguous or cyber risk was not explicitly excluded, coverage is embedded in the policy. In addition, where cyber coverage is present in traditional policies, insurers may not have allocated premium to the exposure.

In addition to silent cyber exposures embedded in many traditional P&C policies, ongoing cyber-related insurance litigation is an obstacle to assessing true cyber exposures. In February 2018, the UK, US and several other countries attributed the NotPetya cyberattacks to the Russian government and its efforts to destabilize Ukraine. A pair of closely watched legal cases are addressing the issue of whether the war exclusion in most traditional P&C policies applies to cyberattacks (see highlight box below). In the cases below, cyber coverage was embedded in traditional P&C policies, and insurers are denying coverage based on the policies' war exclusions, which were written decades ago. The insurance industry is closely monitoring the courts' interpretations of the specific language in the individual contracts because it will help clarify the scope of cyber coverage within traditional policies. These cases also demonstrate that collecting on claims can be a lengthy process depending on complexity, specific policy wording and coverage triggers.

High-stakes legal cases around war exclusions highlight affirmative cyber coverage in traditional P&C Policies

Merck & Co

On August 2, 2018, Merck & Co., Inc. filed a lawsuit in the Superior Court of New Jersey against dozens of its P&C insurers and reinsurers seeking damage under an all-risk property policy seeking coverage in connection with the June 2017 NotPetya attack. In its 2018 10K, the company disclosed around $700 million in costs associated with the attack, citing disputes around the availability of some insurance coverage. According to the complaint, the property policies included physical loss or damage to property, including destruction, distortion or corruption of computer data, coding, program or software; business interruption; extra expenses; expenses to reduce loss; research and development expenses; finished stock and merchandise for sale; extra costs to temporarily continue the movement of goods and materials; and loss adjustment expenses. In March 2018, certain insurers and reinsurers, but not all, reserved the right to deny coverage on grounds that the NotPetya attack was an act of war or terrorism and excluded from coverage. In its complaint, Merck disclosed that it also had privacy and network liability insurance policies (for example, cyber) that cover losses and damages from the event, and that the insurers on the cyber policies have been making payments to Merck, and have not been named as defendants in the action.

Mondelez International, Inc.

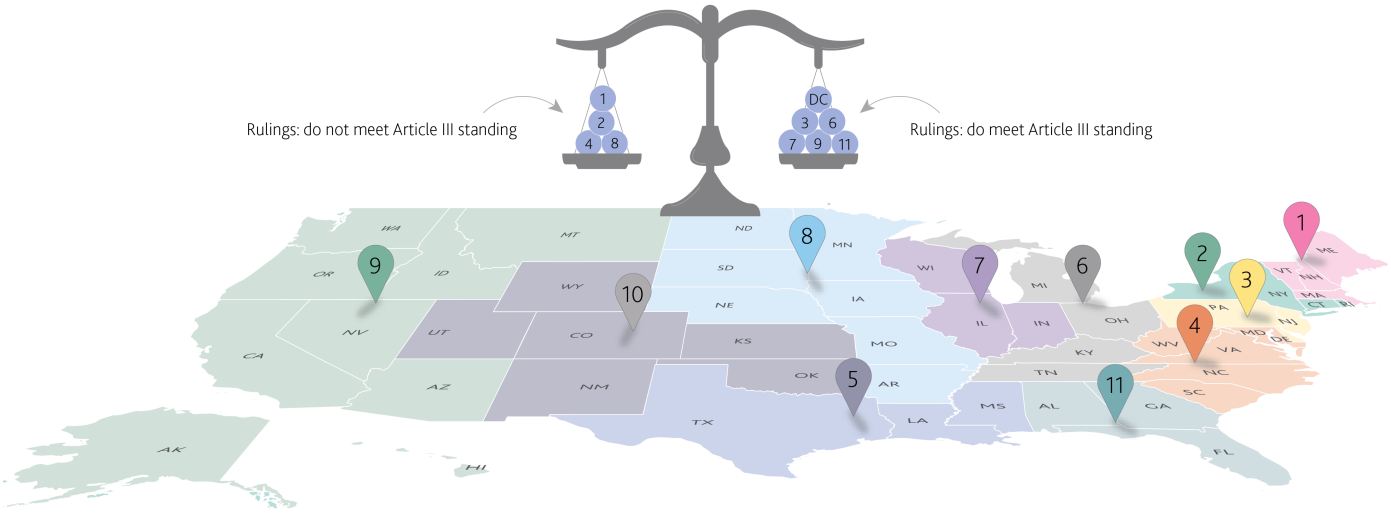
On October 10, 2018, Mondelez International, Inc. filed a lawsuit in the Circuit Court of Illinois against Zurich American Insurance Company seeking damage under an all-risk property policy in connection with the NotPetya attack. According to the complaint, the property policies included "physical loss or damage to electronic data, programs, or software, including physical loss or damage caused by the malicious introduction of a machine code or instruction." The policy also included affirmative cyber coverage as well as "time element" or business interruption and extra expenses. In a June 1, 2018 letter, Zurich denied coverage based on a single policy exclusion that provides: the policy excludes loss or damage directly or indirectly caused by or resulting from any of the following regardless of any other cause or event, whether or not insured under this policy, contributing concurrently or in any other sequence to the loss: hostile or warlike action in time of peace or war, including action in hindering, combating or defending against an actual, impending or expected attack by any: government or sovereign power (de jure or de facto); military, naval, or air force; or agent or authority of any party specified above.

Litigation claims winding their way through the courts; federal circuit courts split

Other ongoing litigation deals with which parties under Article III of the US Constitution can sue for damages from cyberattacks that result in the theft of personal information. Damages can often include legal defense costs that would be paid in part by P&C insurance depending on the policy. Over the past several years, cyber litigation has been winding its way through US federal circuit courts. In its decision on a landmark May 2016 case, *Spokeo, Inc. vs. Robins*, the Supreme Court held that an injury must be both "concrete and particularized" and "actual or imminent, not conjectural or hypothetical" for a plaintiff to have legal basis under Article III. Following that decision, federal appeals courts have been split on whether plaintiffs in cyber damage related cases can proceed to trial. According to several law firms[2], the D.C., Third, Sixth, Seventh, Ninth and Eleventh Circuit Courts have ruled that risk of future harm (for example, identity theft fraud) from a data breach meets Article III standing, while the First, Second, Fourth and Eighth Circuit Courts have held that the risk of future harm does not meet Article III injury requirements (see Exhibit 3).

Exhibit 3

Federal appeals courts are divided on Article III standing in data breach cases



Source: Moody's Investors Service

Underwriting and risk management projects begin to address silent cyber exposure

Insurers are in various stages of assessing and quantifying their true cyber exposure, including silent cyber. This is a top priority for the industry because commercial property exposure limits are often multiples of limits provided by standalone cyber policies. Insurers' actions include creating an inventory of traditional policies with embedded cyber exposure, modifying policy terms and conditions, and allocating premiums to policies that contain cyber risk. Although the market is evolving, insurers that write large national and multinational property accounts are shifting cyber risk to standalone policies or implementing cyber sub-limits, or both. Insurers and reinsurers are also working with third-party vendor modeling firms to help dimension the risk.

Insurers continue to run deterministic scenarios and take underwriting actions, and use reinsurance to manage gross exposure. In April 2019, Allianz announced [3]that it had developed an underwriting strategy to address silent cyber exposures. Allianz's large commercial business unit, AGCS, is taking the lead to implement a strategy for new business that will clarify whether cyber risk is explicitly included in traditional policies or covered in a specific cyber policy. The company also plans to implement a strategy for renewal business, subject to regulatory and filing requirements in certain jurisdictions. Other Allianz companies will implement the strategy by January 2020.

Regulators are also weighing in on silent cyber. On January 30, 2019, The Bank of England Prudential Regulation Authority announced the results of a follow-up survey on cyber underwriting risk. Since publishing its cyber insurance underwriting risk report in 2017, the regulator outlined that it expected insurers to develop action plans by the first half of 2019 with dates and actions taken to address silent cyber risk.[4]In July 2019, Lloyd's of London announced that beginning in 2020, all first-party property policies should be clear as to

whether cyber is or is not covered. For liability and treaty reinsurance, insurers will need to clarify whether cyber is covered in a staged approach in 2020 and 2021. Lloyd's also requires its syndicates to run realistic disaster scenarios, including a major data cyber security breach.

Unique difficulties remain for underwriting cyber insurance

A number of unique challenges remain in underwriting cyber insurance. Although risk modeling for the exposure has advanced, underwriters still struggle with complexity and the ever-changing nature of the risk. The loss-frequency and loss-severity dynamic of cyber risk has more in common with terrorism or crime and fidelity perils than with a fortuitous cause of loss (a loss that occurs that an insured cannot be held to have anticipated).

Expanding analyzable data sets. Insurers have gradually gained experience from continued cyberattacks and through increasing disclosure requirements for publicly traded corporations. However, historical loss information is limited and public disclosures still lag and lack consistency. Loss scenarios supporting cyber underwriting are largely based on known or perceived vulnerabilities and modes of exploitation, all of which evolve.

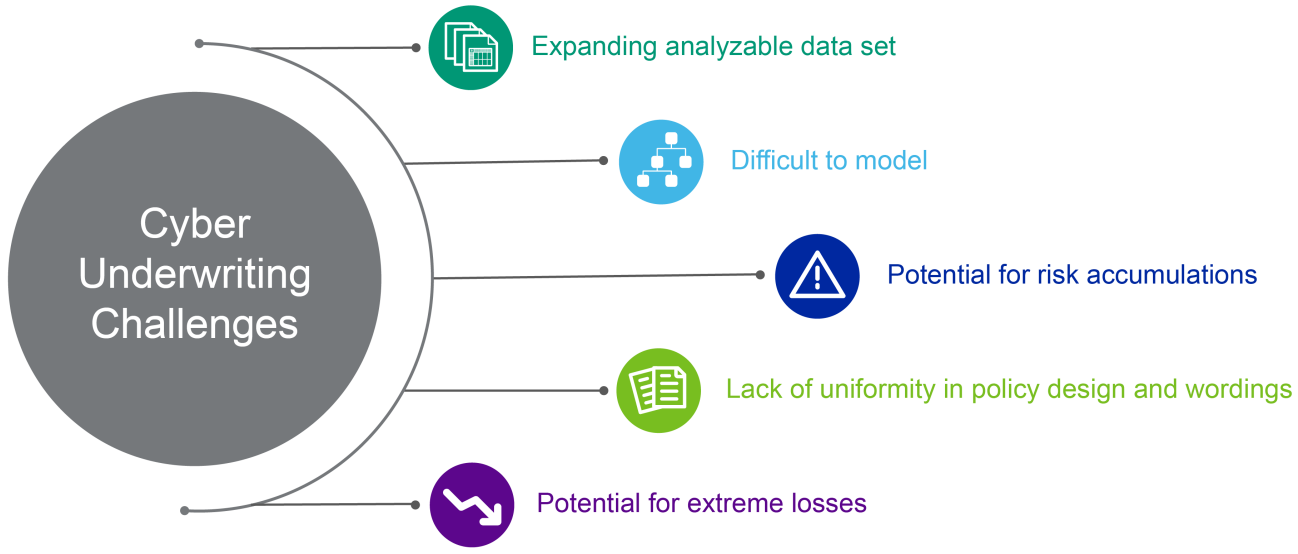
Modeling advances, but still in early stages. Insurance brokers and modeling agencies have been developing cybersecurity probabilistic models (for example CyberCube, Cyence, Risk Management Solutions, Air Worldwide).

Also, Property Claim Services has expanded its industry loss index and estimates service for the cyber insurance segment by adding cyber catastrophe events. The index product now covers losses that involve multiple insureds across affirmative and silent cyber with industrywide insured losses of at least $250 million.

As these models evolve, they provide additional insights into the nature of insurers' underwritten exposures. However, we believe the evolving nature of the risk creates a moving and shifting target for models' parameters.

Exhibit 4 shows the factors that make cyber risk insurance underwriting inherently difficult. Insurers have responded to these complicating factors by using a combination of approaches to manage it, including limits management, assessing aggregations and modeling deterministic and more recently probabilistic scenarios. They also use reinsurance, primarily quota shares, to manage underwriting exposures.

Exhibit 4
Unique underwriting challenges present risks for insurers



Source: Moody's Investors Service

Potential for risk accumulations across multiple insured clients and products. The potential for risk accumulations can result in outsized liabilities for insurers, given that the same loss can affect multiple insured clients. As an example, selected industries may have

a concentration with one or two third-party vendors that provide services to many participants within an industry. Risk accumulation across products is also a potential problem since some cyberattack scenarios can trigger losses across multiple coverage types (e.g. property, general liability, directors' and officers' liability).

Policy design and wording lack uniformity. Underwriters generally seek differentiation rather than uniformity in writing cyber insurance given the unique characteristics of the risk. This leads to variations in product design, wording and coverage triggers across the industry, resulting in challenges to standardized modeling and pricing.

Potential for extreme losses raises question of insurability. The potential severity of gross losses from cyber events is another challenge. The Cyber Risk Management (CyRiM) Report 2019,[5] presents hypothetical scenarios in which malware threatens to destroy or block access to files and spreads around the globe. The report was co-written by Lloyd's, Aon Centre for Innovation and Analytics, MSIG, and SCOR TransRe. Its scenarios result in global economic damages of $85-$193 billion with insured damages including affirmative and silent cyber losses of $10-$27 billion. The CyRiM report places the insurance premium at $6.4 billion, which indicates that insurers' losses would be multiples of the premium from this type of event.

The US Terrorism Risk Insurance Program Reauthorization Act of 2015 (TRIPRA) does not explicitly exclude cyberattacks as a cause of loss for covered exposures. Therefore, we believe that property damage and/or bodily injury losses from a large-scale cyberattack would likely be covered under the program; however, losses from data breaches would most likely not be covered. TRIPRA is scheduled to expire at the end of 2020, although we expect Congress to consider reauthorizing it as that date approaches. Any such reauthorization would likely shift more risk to insurers, as has occurred in the past.

Moody's related publications

Sector research

- Cross-Sector — Global: Credit implications of cyber risk will hinge on business disruptions, reputational effects
- Healthcare — US: Data breach at Quest and LabCorp highlights cyber risk in vendor relationships
- Higher education — Global: Cybersecurity poses a growing credit risk in higher education
- Cyber Insurance: High-Risk Product With Potential to Grow
- Electric and gas – US Pipeline cybersecurity standards help plug security loophole in utility supply chain
- Defense – US Greater cybersecurity accountability for defense contractors would be credit negative
- Higher education – Global, Cybersecurity poses a growing credit risk in higher education
- Financial Institutions – Europe, European financial authorities recommend cybersecurity legislation, a credit positive for financial institutions
- Insurance - Global: (Re)Insurers step up tech investment as disruption threat grows
- Regulated electric and gas utilities - US: Cyber risk is on the rise, but the likelihood of government relief is high
- Banking: Chile issues new cybersecurity regulations, a credit positive for banks
- Local government – Washington: Washington State cybersecurity audits help mitigate risk from growing threat
- Banking: Data-sharing partnerships between technology-enabled firms and big US banks would be credit negative for regional banks
- Banks: Russian central bank's additional capital requirement for banks' cyber risks would be credit positive
- Public power electric utilities - US: Growing grid interconnectivity increases cybersecurity risks
- Asset Managers - US managers sharpen their focus on cybersecurity
- Banks - US: Cybersecurity will improve under new requirements of New York regulator
- Insurers - US and Canada: Survey: North American insurers step up cybersecurity initiatives
- Utilities remain vulnerable and attractive target of cyber attacks, a credit negative

Issuer research

- Equifax Inc. Data breach-related settlements are consistent with our expectations
- British Airways, Plc British Airways faces record-breaking data privacy fine, a credit negative
- Marriott International, Inc. Marriott announces the UK Information Commissioner's Office's intent to issue fine related to Starwood breach
- Medical Products & Devices – US Warning on certain Medtronic insulin pumps highlights cyber risks for medical devices
- Desjardins Group Privacy breach is credit negative for Desjardins Group
- Healthcare - US Data breach at Quest and LabCorp highlights cyber risk in vendor relationships
- First American Financial Corporation Reports unauthorized access to customer data, investigation underway
- Baltimore (City of) MD Second ransomware attack in 15 months disrupts Baltimore's operations

- Equifax Inc. Cybersecurity investments, lagging operating performance and debt-funded M&A to weigh on metrics
- Equifax Inc., Updated credit analysis following revision of rating outlook to negative
- Moody's affirms Equifax sr uns at Baa1, revises outlook to negative from stable
- Los Angeles Harbor Department, CA Cybersecurity working group is a credit-positive step to address threats
- Matanuska-Susitna (Borough of) AK, Quick, coordinated response, access to emergency funds and insurance limit cyberattack losses
- Norsk Hydro ASA, Severe cyberattack forces operations into partial manual mode, a credit negative
- Marriott announces credit-negative data security incident
- SBM Bank (Mauritius) Ltd. Cyberfraud at SBM Bank's Indian branch highlights international operational risks, a credit negative
- Tesco Bank fined £16.4 million for 2016 cyberattack, a credit negative
- Envigo Laboratories Inc.: Update to credit analysis following downgrade of CFR to Caa2
- BMO and CIBC suffer a credit-negative customer data privacy breach
- Equifax: Continuing fallout from cybersecurity breach will erode profitability in 2018 and litigation risks will remain high
- FedEx Corporation: Update to credit analysis - Expected deleveraging remains on track
- Equifax's security breach is credit negative but Baa1 rating unaffected
- Merck & Co.: Credit negative cyber-attack is mitigated by positive business fundamentals

Topic page

- Cyber Risk

To access any of these reports, click on the entry above. Note that these references are current as of the date of publication of this report and that more recent reports may be available. All research may not be available to all clients.

Endnotes

1 Ponemon Institute 2019 report, **Ninth Annual Cost of Cybercrime Study: Unlocking the Value of Improved Cybersecurity Protection**

2 Cleary, Gottlieb: **Supreme Court Declines to Review Standing in the Data Breach Context Despite Ongoing Circuit Split**, March 7, 2018; Mayer Brown: **2019 Outlook Cybersecurity and Data Privacy**

3 Allianz Global, "**Making noise about 'silent cyber**'"

4 Bank of England Prudential Regulation Authority, **Cyber underwriting risk: follow-up survey results**, January 30, 2019.

5 **Bashe attack: Global infection by contagious malware**

REPORT NUMBER 1147603

Contacts

Sarah Hibler +1.212.553.4912
Associate Managing Director
sarah.hibler@moodys.com

Mohnish Pardasani +1.212.553.3899
Associate Analyst
mohnish.pardasani@moodys.com

CLIENT SERVICES

Americas	1-212-553-1653
Asia Pacific	852-3551-3077
Japan	81-3-5408-4100
EMEA	44-20-7772-5454

MOODY'S
INVESTORS SERVICE