Insuring Cyber Risk

AN AIR ISSUE BRIEF

What is holding cyber insurance back, and how can the industry push forward?

AIR

Cyber risk is fast becoming a top-of-mind concern for risk managers across all business sectors. Organizations large and small are investing in risk and loss mitigation, including preventative security and post-event recovery measures. Accordingly, cyber insurance represents one of the fastest growing sectors of the insurance industry, driven in no small part by a spate of high-profile incidents in recent years (see table on next page).

Premiums in 2016 totaled approximately USD 3.25 billion according to the Insurance Information Institute, up from 1 billion just five years ago. Still, in the context of how many businesses worldwide can be affected by cyber attacks and the potential scale of the losses, the market is considered nascent.

The continued expansion of the cyber insurance market is both necessary and inevitable, but the path to growth is uncertain. Will it take an extreme aggregation event, the cyber equivalent of a Hurricane Andrew, to serve as a wake-up call to the insurance industry? Or will proactive stakeholders lead the way to a stable, risk-based cyber insurance ecosystem, ahead of the next truly catastrophic event?

This paper looks at some of the primary challenges facing cyber insurance today and how industry leaders armed with the tools needed to confidently assess the risk can move this market forward.

FORECAST CYBER INSURANCE PREMIUM VOLUME BY 2025 (SOURCE: ALLIANZ GLOBAL CORPORATE & SPECIALTY)

INCREASE IN CYBER INCIDENTS FROM 2015 TO 2016 (SOURCE: IDG)

MAJOR CYBER INCIDENTS IN THE PAST FIVE YEARS

Date	Target	Impact
2013	Target	Data breach exposed debit and credit card accounts of 40 million customers, followed by an additional breach affecting 70 million customers
2014	Sony	Hack immobilized the company's computer, email, and voicemail systems, and leaked confidential files and Social Security numbers
2014	Home Depot	Data breach compromised email or credit card information of more than 50 million customers.
2015	Anthem	Medical data breach resulted in 80 million records stolen.
2016	Dyn	Distributed denial of service attack on domain name system provider Dyn shut down many of the world's most popular websites (including Twitter, Spotify, GitHub, Netflix, and CNN) for several hours.
2017	Amazon Web Services (AWS)	A typo by an AWS employee led to inadvertent shutdown of parts of AWS for several hours.
2017	Hundreds of thousands of computers in more than 150 countries	The WannaCry ransomware attack exploited a known vulnerability in older Windows operating systems, encrypting files and demanding a ransom to be paid for the decryption key.

What Is Holding Cyber Insurance Back?

While awareness of the risk of cyber attacks is rising, the penetration of cyber insurance is estimated at less than 30% in the United States (where almost 90% of premiums are currently being underwritten). On the demand side, buyers often do not have a good grasp of how much cyber risk they face and are wary of limited, often expensive coverage. And it is difficult for buyers to compare coverage or pricing as there is no widely accepted "standardized" cyber insurance policy form language yet in the marketplace (although **the enhanced program from ISO** is aiming to change that).

Still, the demand for cyber insurance currently outpaces capacity, and many buyers cannot obtain sufficient coverage, especially without adopting costly and unrealistically stringent IT requirements, like limiting the number of records stored. Furthermore, most cyber policies today cover the direct cost of breaches and third-party liability, while business interruption and contingent business interruption coverage are less common.

It is clear that there is much room for growth, but without the tools to confidently quantify the risk, most insurers do not see a clear path to *profitable* growth. Here are some of the primary challenges facing the market today.

Insurers Are Mired in the Cyber Gray Area

The lack of standardization can present several difficulties for many insurers. In the aftermath of an event, insureds might seek coverage under cyber liability policies—which underwriters may not have taken into consideration when pricing these insurance products.

Another possibility is having to pay out cyber-related losses under non-cyber policies, known to many in the industry as "silent cyber." If an insured has a loss, they may try to "find" coverage under their other policies, such as (but not limited to) errors & omissions (E&O), directors & officers (D&O), commercial crime, or commercial general liability (CGL).

With cyber policy language largely untested today in the courts, different jurisdictions possibly taking different approaches to coverage disputes that arise, and cyber-related losses and claims accelerating, insurers and reinsurers are well advised to take a very close look at how they manage cyber risk that they intend to insure, as well as cyber risk that they don't intend to insure.

In the examples below, depending on the underlying facts of the claim, the specific language of the policy provisions at issue, and the legal landscape of the jurisdiction involved, the cyber-related event might result in a claim under a cyber policy or under any of the more traditional policies such as CGL or D&O.

- An employee wired money to an account, wrongly believing that the individual who told him to do so through social media was his boss
- Business interruption from a business's lack of access to a hacked credit card processing vendor (where no breach may have occurred at the insured company)
- Loss of sensitive customer data
- A part-time hospital employee gained unauthorized access to confidential records and discussed HIPAA sensitive information with others
- Lost laptop with sensitive information

Data Scarcity Makes for Fuzzy Math

A major element affecting many insurers' willingness and ability to write cyber risk is the relative scarcity of reliable data on incidents and losses. Cyber constitutes high severity risk like the natural perils that catastrophe models were created to address, although unlike natural catastrophes, cyber events are frequent and becoming more so, though many are not severe). However, the necessary inputs for creating a reliable cyber model have traditionally been sparse, non-standardized, and often proprietary.

Furthermore, the historical record for cyber breaches is comparatively short, many attacks go undetected and unattributed, and many companies are hesitant to publicize that they have been breached unless required by law. Finally, the constantly evolving nature of the risk makes it all the more challenging to use past events to project future losses, while the human element in cyber attacks adds to the uncertainty. Cyber criminals are becoming more sophisticated, and the ever-expanding internet of things is broadening the range of possible targets.

Spotty Exposure Data

A data scarcity problem is present in underwriting as well, for different reasons. Before a contract is signed, there is a delicate balance between collecting enough appropriate information on the potential insured's risk profile and requesting too much information about cyber vulnerabilities that the insured is unwilling or unable to divulge. Many insurers might only require the industry and revenue of a potential insured, while others may spend weeks interviewing IT staff and require comprehensive questionnaires to be filled out before deciding whether the risk fits with the portfolio's underwriting guidelines. In addition, there is the difficult challenge of shadow IT (applications

deployed by business unit personnel) and internet-facing infrastructure, which the IT department has no visibility into.

Unlike property risk, there is still no standard set of exposure data that is collected at the point of underwriting.

Without sufficient claims data to correlate risk factors with actual losses, cyber underwriting and pricing today tends to be more art than science, relying on many subjective measures to differentiate risk.

The Bottom Line

Taken together, these challenges have restricted the size of the cyber insurance market. Without full understanding of how much risk they are taking on, and wary of the very real possibility of extreme risk accumulation from unknown portfolio correlations, many insurers set relatively low limits and a multitude of exclusions to try to control their potential losses, in addition to high premiums. Methods currently used for managing accumulations, based on estimated market share, can offer a crude assessment of the risk, but miss the mark more often than not.

At the same time that many insurers are holding back, others are jumping in with cyber offerings (both endorsements and standalone policies) to attract customers in a highly competitive and soft market, but without sufficient tools to measure the risk. Regulators are taking notice.

Reinsurers also recognize cyber as an important growth opportunity, but many are likewise wary of the potential of accumulating extreme losses. Like the primary market, the reinsurance market is struggling to develop robust solutions for managing and mitigating these risks. One challenge is that reinsurance treaties often lack appropriate exclusions for cyber risks, as some clients and brokers are unwilling to accept exclusions in a highly competitive marketplace. Even when exclusions are included, they may quickly become obsolete given the rapidly evolving nature of the risk.

What Does Sustainable Cyber Risk Management Look Like?

Effective management of cyber risk requires the ability to bridge the disconnect that currently exists between exposure and loss potential. This requires an objective understanding of the exposure and the ability to differentiate exposures based on their cyber vulnerability, the ability to monitor accumulations and set underwriting guidelines, a robust way to estimate losses across many lines of business, and transparent and efficient ways to transfer risk.

Reliable, Standardized Data

First and foremost, better cyber risk management can only come about when the industry adopts a shared language when talking about the exposure. This will help underwriters differentiate risk based on commonly understood data elements, and facilitate the transfer of risk through the insurance value chain.

AIR developed the Verisk Cyber Exposure Data Standard in consultation with more than 60 companies in the cyber insurance, broking, reinsurance, and security spaces. An open source, cross-market initiative, the standard was released to the public in January 2016.

Effective management of cyber risk requires the ability to bridge the disconnect that currently exists between exposure and loss potential.

Descriptions of the broad categories of data elements are provided in the table below.

The data standard was designed to accommodate whatever exposure information might be available. Some insurers might have only the industry and revenue of a potential insured, while others collect more detailed information, such as the identities of cloud service providers and number of data records held by the company.

Of course, the more detailed the input information, the more accurate the risk assessment will likely be. To this end, AIR can augment missing exposure data using a unique, detailed database of company-specific information for tens of thousands of global commercial establishments. The database can be used to fill in missing information on an insured's revenue, number of employees, number of data records, replacement cost per record, business interruption cost, and service providers.

VERISK CYBER EXPOSURE DATA STANDARD: AN OVERVIEW

Organization	The nature of an insured's cyber risk is first characterized by its size (in terms of revenue) and the industry in which it operates. In fact, these are the only two fields that are required by our model to perform a cyber risk analysis. Additional information includes the organization's demographics and the quality of its cyber security and recovery plans.
Data	The type of data assets held by the insured—intellectual property, credit card information, health records, etc.—may determine potential financial losses if they become lost, stolen, or unavailable as a result of a cyber incident.
Storage	Data is at risk when it is stored on devices such as servers, laptops, flash drives, or mobile devices. These data storage locations have different vulnerabilities and security features that are factors in determining cyber risk. Significant risk can aggregate as more and more data is concentrated in the cloud. Cloud providers can be captured in the standard.
Transfer	How data is transferred between and within organizations leads to additional vulnerabilities that can result in breaches, even if storage sites are protected with high quality measures such as encryption. Data transfer mechanisms such as email, point-of-sale networks, web applications, and others are all captured in the standard.
Insurance Terms	The financial component of the standard defines how economic losses from a cyber event are translated into insurance gross losses. Multiple insurance contract types—such as standalone cyber liability, cyber liability endorsement, general liability coverages, errors and omissions coverages, and non-physical damage business interruption—can be captured. The breadth of coverages supported allow insurers to model losses associated with data destruction, denial-of-service attacks, theft and extortion, incident response and remediation, crisis management, forensic investigations, data restoration, business interruption, and others.

Flexibility to Accommodate Evolving Coverages

Flexibility was a key goal in creating the Verisk Cyber Exposure Data Standard to help it be applicable across the entire spectrum of cyber risk underwriting, and any organization (including businesses, non-profit organizations, and governments) can be represented using the standard.

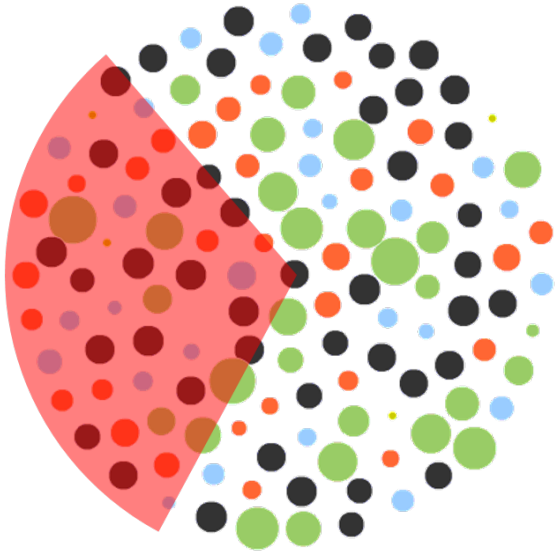
In the absence of standardized cyber coverages and policy form wording, the Verisk Cyber Exposure Data Standard allows an insurer to specify cyber perils and policies relevant to their offerings, rather than make broad-brush assumptions about what is applicable. Any cyber-related loss can be mapped to any policy protection form offered in the Verisk Cyber Exposure Data Standard—including cyber, E&O, D&O, CGL and more. Policies that inure to the benefit of other policies, sublimits, and other financial vehicles are also supported.

Accumulation Management

The aggregate nature of cyber risk means that numerous organizations can suffer simultaneous financial losses if a common service provider is accidentally or maliciously breached. The October 2016 distributed denial of service (DDoS) attack on Dyn, a domain name system provider, is a recent example of the potential for extreme risk aggregation. The attack resulted in downtime for some of the world's top websites, including Netflix, Paypal, Reddit, CNN, and Twitter. Business interruption losses were limited, however, because most policies require an 8- or 12-hour waiting period "deductible." The Dyn service interruption was resolved in far less than this.

Cyber accumulations are notoriously difficult to manage because the interconnectedness of the companies within a portfolio is often hidden. For a typical insurer today, it is not uncommon for information beyond an insured's industry, revenue, and company name to be unknown. In fact, many insurers who write volume business may not even know the insured's name, but only the industry and revenue. As a result, a market share approach is often used to accumulate risk and to conduct scenario analyses.

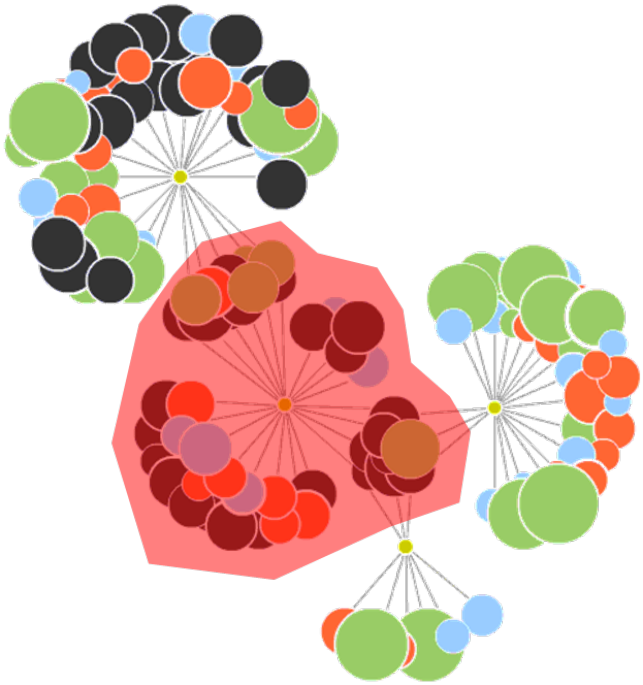
To estimate the risk accumulation around a cloud provider, for example, an insurer might assume that the cloud provider's market share is exactly reflected among the companies in the portfolio. In other words, that same percentage of companies in the portfolio would be at risk of suffering losses if the cloud provider experienced downtime.



IN THIS DEPICTION OF A PORTFOLIO, EACH BUBBLE REPRESENTS AN INDIVIDUAL COMPANY, THE COLORS REPRESENT DIFFERENT INDUSTRIES, AND THE SIZE OF THE BUBBLE REPRESENTS THE COMPANY'S REVENUE. USING A MARKET SHARE APPROACH, ONE MIGHT ASSUME THAT THE REGION IN RED ENCOMPASSES THE COMPANIES AFFECTED, SHOULD A CLOUD PROVIDER WITH A 33% MARKET SHARE EXPERIENCE DOWNTIME. (SOURCE: AIR)

Risk managers recognize that this method is rife with imprecision, so they may opt to repeat the process by sampling different segments of the portfolio to obtain a distribution of modeled losses. However, without knowledge of the insureds' actual service providers, there is a good chance that the market share approach will under- or overestimate accumulation risk. In fact, in one study, AIR found that approximately 80% of portfolios do not match the results of a market share approach when it comes to third-party service providers.

Fortunately, these and other important data for modeling cyber risk are available through AIR's database of industry exposures. Informed by specific data on each company's suppliers, the portfolio can be organized around the source of risk being analyzed. This detailed accumulation approach provides a far more accurate view of the risk than the market share approach because it identifies only the exposures that would actually be affected and omits those that should not be considered.



THIS IMAGE PORTRAYS THE SAME PORTFOLIO AS BEFORE, BUT BECAUSE IT REFLECTS COMPANY-SPECIFIC DATA ON PROVIDERS, THE REGION IN RED INDICATES THE COMPANIES KNOWN TO BE RELIANT ON THE CLOUD VENDOR AFFECTED BY A DOWNTIME EVENT. (CLOUD VENDORS ARE INDICATED BY THE SMALL YELLOW NODES.) (SOURCE: AIR)

Robust Scenario Modeling

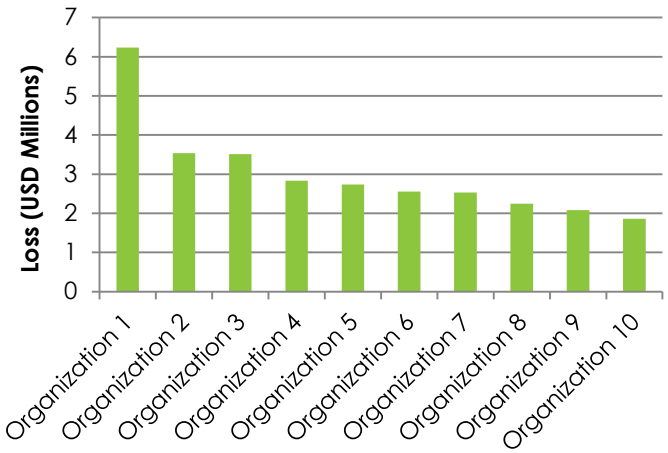
With the foundation of sound exposure data and the ability to confidently accumulate risk, the next step to understanding cyber risk is to model the financial impact of various breach scenarios.

AIR's Analytics of Risk from Cyber (ARC) application was released in April of 2017. ARC enables organizations to manage their cyber exposures, augment their data using AIR's proprietary database of industry exposures, and calculate losses from 18 types of deterministic scenarios. Each one can easily be modified to change the target companies, severity of the attack, cost assumptions, and policy coverage assumptions to yield an unlimited number of bespoke scenarios. Insurers can use scenario modeling to identify single points of risk aggregation to inform their reinsurance purchasing and underwriting decisions.

Depending on the makeup of portfolio, high impact scenarios can include one or more of the following.

SECURITY BREACH

Data theft from malicious or unintentional security breaches have been some of the most publicized forms of cyber incidents to date. Types of data at risk include credit card numbers, names, emails, passwords, health or financial records, and intellectual property. Hackers use a variety of techniques to steal these data, including social engineering, phishing, and deploying malicious internal agents.



SAMPLE MODELING RESULTS FOR ACCIDENTAL DATA BREACH SCENARIO, LOSSES BY ORGANIZATION (SOURCE: AIR)

Breaches can result in direct losses when intellectual property is stolen, data are destroyed, operations are interrupted, or systems suffer physical damage. Indirect losses can include third-party liability from the compromise of proprietary data and

reputational losses. One particularly attractive target for cyber criminals is a credit card payment processor/acquirer. A successful attack could yield millions of credit card numbers. For an insurer, the financial consequences could be catastrophic.

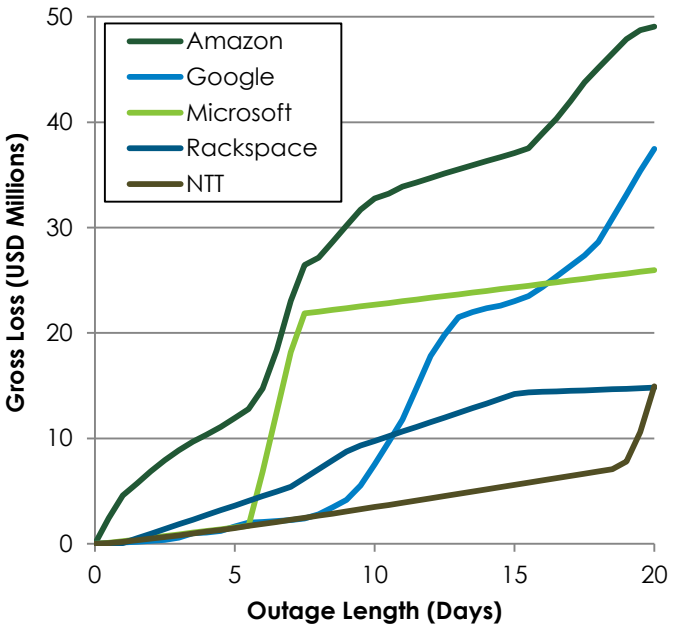
Furthermore, breached companies can face heavy fines for inadequately protecting customer data. As of mid-June 2017, 48 of the 50 states in the United States require some form of breach notification. And beginning in May 2018, new regulations will require notifications in the European Union, as well.

BUSINESS INTERRUPTION

Business interruption (BI) losses result when a company experiences a disruption to its operations as a direct result of a cyber event, and contingent business interruption (CBI) losses result when a company suffers downtime because its vendor or supply chain is affected by a cyber event. Both are time-element coverages that compensate the insured for lost business revenue and operational costs associated with the disruption.

Cyber-related BI can have a pronounced effect on a wide variety of industries, including manufacturing, retail, and transportation. CBI can have an even wider impact because most organizations rely on third-party vendors for part of their operations. If a service provider experiences downtime because of a breach, many of their customers can suffer simultaneous losses. Cloud service providers are a particularly worrisome point of aggregate risk, as the top five own more than half the market. Other scenarios that could result in BI and CBI losses include attacks on a payment processor, domain name system provider, email server, content delivery network, or ad network.

For all scenarios available in ARC, the user can model disruption to a comprehensive selection of providers and specify the number of days or hours of interruption, including a range of days.

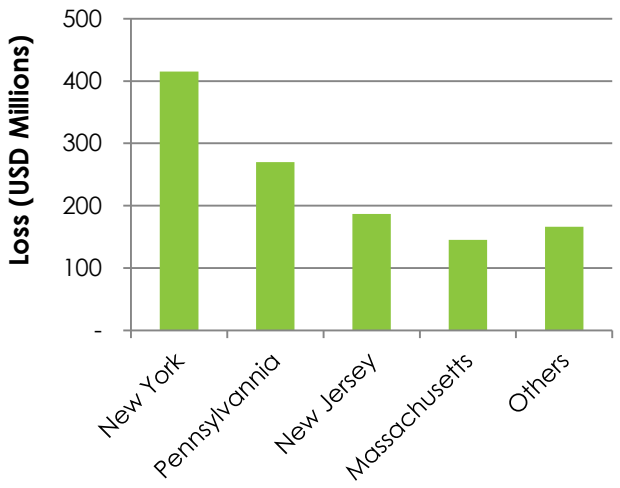


SAMPLE MODELING RESULTS FOR CLOUD BREACH SCENARIO, LOSSES BY PROVIDERM (SOURCE: AIR)

BLACKOUT

An attack on the power grid, which is run by a utility that drives electricity through a common network of power lines, could lead to business interruption losses across a large geographic area. While no blackout in the U.S. or U.K. has yet been publicly attributed to a cyber attack, it has happened in the Ukraine, demonstrating that the types of malware and viruses capable of causing a blackout already exist.

In August 2016, Lloyd's required its syndicates to provide their estimates of the 100% industry insured loss in relation to eight cyber attack scenarios, including two blackout scenarios, one in the U.S. and one in the U.K., each with three levels of severity. AIR's implementation of the scenarios identifies geographic areas of recovery and the duration of the power outage for each area. Business interruption losses can be calculated based on the locations of the organizations in a portfolio.



SAMPLE MODELING RESULTS FOR NORTHEAST U.S. BLACKOUT SCENARIO, LOSSES BY STATE (SOURCE: AIR)

Up Next—Underwriting Solutions

Scenario modeling provides a sense of how severe the losses can be from a cyber attack, but additional information is often needed to select and price individual risks. Verisk Analytics is seeking to address the challenge of understanding risks at the point of underwriting with the launch of a cyber insurance program and the development of a platform that provides comprehensive cyber risk data for millions of organizations.

In addition, AIR is actively working on a probabilistic cyber model that will be available in an upcoming release of ARC. The probabilistic model will help companies understand the impact and likelihood of data breaches and various large aggregation events.

The Way Forward

Thanks to the rising awareness of the risk of cyber events, the penetration of cyber insurance is increasing, although there is still considerable room for growth. Improving insurance take-up will help businesses and communities become more resilient to the potentially catastrophic impact of cyber-related losses. While larger companies may have reserves and loss response measures to weather an attack, small and medium enterprises can easily go out of business without the essential protection that insurance can afford. In fact, many underwriters offer incident response services that help companies in the aftermath of an attack to resume business operations as quickly as possible, including eradicating viruses, notifying stakeholders, and improving customer and public relations. Insurance can also incentivize companies to improve their cyber security measures by way of risk-based premium reductions, much like mitigation discounts work for property owners.

Of course, it is not only corporations that are at risk. Hospitals, utilities, transportation, and other critical infrastructure can be targeted, with alarming impact to communities. Recognizing the potentially catastrophic impact of such attacks, the EU has recently signed new legislation that requires the providers of essential services to report incidents and demonstrate sound cybersecurity measures. Notably, the classification of "essential services" includes not only infrastructure, healthcare, and financial institutions, but also cloud and search engine providers, a testament to today's significant reliance on digital services and interconnected technologies. The legislation, called the **General Data Protection Regulation**, or GDPR, takes effect in May 2018 and is expected to significantly drive up demand for cyber insurance in Europe.

Among most insurers, there is widespread recognition of the potential for extreme accumulated losses from a cyber event, be it from an attack on a cloud provider or payment processor, a power grid attack, massive data exfiltration, exploiting a weakness in a commonly used software application, or any one of a number of other nightmare scenarios. Incidents with widespread impact like the Dyn attack in October 2016 and the WannaCry ransomware attack in May 2017 will only become more frequent. A truly catastrophic cyber event has yet to occur, but it is only a matter of time, and many insurers have been hesitant to take a gamble without the proper tools to understand the risk.

While the standardization of cyber insurance is likely years away, the need for effective risk management is evident now. AIR's ARC enables insurers to manage portfolios, assess risk accumulations, and conduct scenario analyses today, while setting them up in an advantageous position to perform probabilistic cyber modeling in the near future.

CONTACT US

If you would like to learn more about cyber modeling, please contact us at **cyber@air-worldwide.com**.

ABOUT AIR WORLDWIDE

AIR Worldwide (AIR) provides risk modeling solutions that make individuals, businesses, and society more resilient to extreme events. In 1987, AIR Worldwide founded the catastrophe modeling industry and today models the risk from natural catastrophes, terrorism, pandemics, casualty catastrophes, and cyber attacks, globally. Insurance, reinsurance, financial, corporate, and government clients rely on AIR's advanced science, software, and consulting services for catastrophe risk management, insurance-linked securities, site-specific engineering analyses, and agricultural risk management. AIR Worldwide, a Verisk Analytics (Nasdaq:VRSK) business, is headquartered in Boston with additional offices in North America, Europe, and Asia.

For more information, please visit **www.air-worldwide.com**.