AIR Cyber Risk Solutions

Your company is exposed to cyber risk—either through the policies you write or through the often invisible interconnectivity of today's home, workplace, and social environments. Do you know what your global cyber accumulations are? More importantly, do you know the consequences of not knowing? What does this ever-growing class of business mean for your enterprise risk? And what opportunities are available in this space?

The Risk

A cyber event that causes simultaneous losses to hundreds of thousands of insureds is the stuff of nightmares, particularly when you consider the variety of scenarios that could give rise to such an event.

If you are writing cyber policies or include cyber coverage in "all-risk" general liability (GL) policies, you could be subject to cyber claims. Whether motivated by regulatory requirements or a desire to gain a different perspective on existing books of business, you know you can't afford to wait for a cyber event to occur to begin managing this risk.

The Opportunity

In today's competitive marketplace, cyber risk is quickly becoming an important growth opportunity. Armed with the right tools, you can channel this complex emerging peril into your company's next success story.

LEVERAGING THE VERISK CYBER EXPOSURE DATA STANDARD

To help (re)insurers understand their cyber risk today, AIR provides products and services to model cyber risk. The Verisk Cyber Exposure Data Standard is the bedrock. Implementing this framework puts your organization on the path toward effective risk management and readies your workflows for the upcoming AIR Probabilistic Cyber Risk Model. Not only will you lay the foundation for future success, but you will also give yourself a tool for analyzing deterministic events and answering critical questions today.

AUGMENTING DATA AND EVALUATING UNDERWRITING GUIDELINES

Exposure data quality will be critical as you move forward; however, the cyber insurance market can be competitive, and insureds will prefer to seek protection while maintaining as much confidentiality about their business as possible. For this reason, the most successful insurers will be those who know the right questions to ask and can augment the answers with data from other sources. AIR understands this and is ready to help you.

AIR already provides consulting services to help underwriters identify the guidelines that will impact cyber risk assessments most. AIR's database of company-specific information for tens of thousands of global commercial establishments can be leveraged to supplement your data with critical information such as cloud provider and employee count. Through these engagements, AIR can transfer your data into the standard format, augment it, and convert it into decision-making assets.

AIR

What Decisions Can AIR Cyber Solutions Help You Make?

UNDERWRITING ACCUMULATION	Define your capacity and continuously monitor cyber risk accumulations. For example, with the Verisk standard you can set limits on the amount of exposure that is found on specific payment processing vendors. Similarly, you can discover which third-party vendors are most heavily utilized within your portfolio of risk.
UNDERWRITING GUIDELINES ASSESSMENT	Companies in the market for cyber insurance are looking to obtain this protection while also maintaining a level of confidentiality about their business operations. This means that competition between cyber insurers also extends to the amount of information they require from insureds. AIR can help you understand the efficacy of your underwriting guidelines for detecting loss potential, giving you the information needed to prioritize what information is captured from potential insureds.
REINSURANCE PURCHASES	As your appetite for cyber risk changes, transferring this risk to reinsurance markets may become necessary. Performing deterministic analyses of extreme but plausible cyber events will let your organization know how much risk needs to be transferred.
COST-BENEFIT AND SENSITIVITY ANALYSES	The Verisk standard includes a Quality Score Rubric to help assess the vulnerability of cyber exposures, but as with any subjective guideline, some uncertainty will be present. To reduce the sources of uncertainty, sensitivity analyses can be performed by adjusting the variables within the standard and comparing the outcomes deterministically. Similarly, cost-benefit analyses can be executed to grade the value of an insured enhancing its security protocols.
RISK MITIGATION	Analysis of network dependencies may reveal significant accumulations of risk associated with third-party organizations such as cloud providers. Insurers may elect to meet with these third-party entities to better understand their impact on an insured's cyber risk. The findings can be used to encourage or require insureds to implement best practices (such as employee training) that reduce risk.
REGULATORY COMPLIANCE	Emerging risks such as cyber are not only of interest to those seeking opportunities for business growth, but also to regulatory entities concerned with ensuring the solvency of the industry. To provide guidance and meet regulatory requirements, re/insurers can analyze the state of their cyber books by performing deterministic analyses. In fact, Lloyd's of London has already mandated syndicates to study a number of cyber scenarios on a regular basis and include those findings in risk appetite and management statements.

Get Answers to Questions About Your Cyber Risk Now

AIR cyber risk consulting services are ideal for companies just starting to look into this emerging peril or for seasoned cyber insurers who can benefit from additional insights. Through this process, AIR can ensure the quality of your data, at whatever level of detail you are able to provide, and produce insightful reports upon which you can base risk management decisions.

By converting your data to the Verisk standard, AIR can leverage information assets from both the Verisk Analytics family and our data partners to augment the data in your book with additional information on network dependencies and a company's demographics—which are often the most challenging points to obtain. All this is possible by providing as little as the names of the organizations in your book. If these aren't available, AIR can use its industry averages to perform studies with industry category and revenue as the only required fields. Additional information, if available, will help refine the risk assessment.

This enhanced exposure data can then be used to perform deterministic scenario analysis. AIR will work with you to identify the scenarios that are most relevant to your business. An assessment of the probability of cyber attack and its loss potential for given industry and company size is also possible, in light of AIR's wealth of data. These custom studies can help you better understand the potential for your portfolio to accumulate cyber event losses. In addition, AIR can help gauge the effectiveness of your underwriting guidelines by judging their performance against our record of over 16,000 historical cyber events and our industry exposure database.

Today and always, AIR is ready to work with you as a trusted and reliable partner to help you achieve your risk management goals. AIR cyber solutions are available now for you to begin managing this growing risk.

Identify and Capture the Right Exposure Data

Cyber coverage is becoming a more important component of an insurer's business, so it's critical that the exposure data being used to assess this risk be complete, of good quality, and standardized so it can be efficiently shared across the insurance value chain. With this issue in mind,

(cont. on page 6)

What Exposure Information Is Captured in the Data Standard?

AIR developed the Verisk Cyber Exposure Data Standard in consultation with our sister company ISO®, which has developed a policy form for cyber risk. In addition, AIR met with more than 60 companies in the cyber insurance, broking, reinsurance, and security spaces and refined the standard with their input.

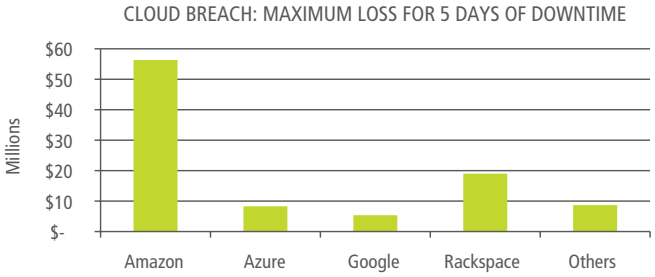
ORGANIZATION	The nature of an insured's cyber risk begins to take shape depending on its size (revenues) and the industry in which it operates. In fact, these are the only two fields that are required to perform a cyber risk analysis. Additional information includes the organization's demographics and 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 it becomes lost, stolen, or unavailable as a result of a cyber event.
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 final component of the standard is the insurance terminology that 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—are included. 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.

What Are Examples of Cyber Scenarios That Can Be Modeled Deterministically?

CYBER DATA THEFT	Data breaches have been the most publicized incidents to date. The types of data that are at risk include names, emails, passwords, health or financial records, and intellectual property. Hackers have been known to use a variety of techniques to steal this data—social engineering, phishing, deploying malicious internal agents, and others—all of which can be modeled with the Verisk Cyber Exposure Data Standard.
VULNERABLE OR UNSUPPORTED SOFTWARE	Hackers are constantly looking for holes within popular software products to exploit. These "zero day" vulnerabilities do not get addressed by vendors when a product reaches its end-of-life point. Despite this risk, many people continue to rely on unsupported products. For example, about 12% of computers around the world still use Windows XP, which is no longer supported by Microsoft. If a new flaw is discovered, it will not be patched, leading to a potential aggregation loss.
ACCIDENTAL CYBER DATA LOSS	The more people an organization employs, the more likely it is that one of them makes a mistake and exposes data. Typically, this scenario consists of mobile devices such as laptop computers, USB drivers, or even a briefcase containing printouts of sensitive information being lost or misplaced. By assigning a probability of an employee losing data, insurers can estimate the associated losses.
DENIAL-OF-SERVICE (DOS) ATTACK	Many hackers are motivated by pride or politics. Their goals are more visibly served by shutting down their victims and those victims' operations than by stealing their data or money. One tactic that these types of hackers use is the denial-of-service (DoS) attack. DoS attacks work by overwhelming a target's network with a massive number of requests, effectively denying legitimate users from accessing the target's services. When lost revenue, incident response costs, or reputational damage occurs, the target can make a cyber insurance claim.
CLOUD SERVICE PROVIDER FAILURE	Companies of all industries and sizes have been outsourcing significant portions of their operations to cloud service providers, but the efficiency benefits gained from this shift do come with a risk. The top five cloud service providers own over half the market. If any of these providers were to experience downtime or a breach, their customers would suffer losses. With the Verisk Cyber Exposure Data Standard, insurers can perform aggregation analyses for their books of business and model the impact of contingent business interruption (CBI) or data record loss resulting from a cloud service provider failure.
PAYMENT PROCESSOR FAILURE	Commercial transactions, for which monetary exchanges are done without cash, are becoming ubiquitous. More businesses rely on payment processing vendors and their network-enabled systems to collect revenue from clients. If a payment mechanism is down, businesses are forced to turn away customers and revenue is lost. Similar to cloud service provider failure, affected companies can claim business interruption losses.
DNS PROVIDER FAILURE	Domain Name Server (DNS) providers manage the systems by which websites receive their addresses and names. Many businesses that want a web presence as a scalable marketing channel rely on DNS providers to keep their websites up and running, and protect them from cyber threats such as viruses and malware. If a DNS provider were to go down, a business interruption loss could result.
CYBER EXTORTION	Cyber extortion criminals threaten to attack an entity's information systems unless a ransom is paid. These hackers could create a sophisticated form of ransomware and target many companies. Cyber extortion victims typically download ransomware by accident when they open or click on links within a malicious email. Afterward their systems become encrypted and the extortionists offer the decryption key in exchange for Bitcoins, a digital currency. Cyber insurance is claimed for the value of the ransom paid.
BLACKOUTS	A blackout can occur for many natural or man-made reasons. Heavy winds, lightning, construction accidents, or scheduled maintenance can all lead to power being lost. During a blackout, companies that haven't implemented mitigation procedures may not have access to their data and can claim business interruption loss. Location data can be used to analyze the loss potential of insureds that lie within that blackout footprint were such an event to occur.

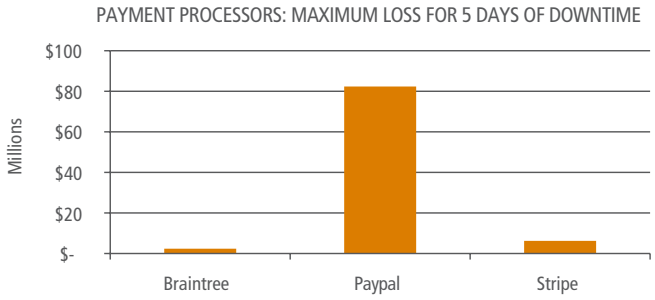
INTERNET SERVICE PROVIDER FAILURE	Equipment failure at a large Internet service provider (ISP) knocks out Internet access for thousands of companies. The small and medium-sized enterprise (SME) sector is perhaps the most impacted, as they make lack the resources to demand high-level service agreements or to employ dedicated in-house teams. During this period of time, affected companies may not have access to data needed to operate their business and can claim business interruption losses.
PUBLIC KEY INFRASTRUCTURE COMPROMISE	A public key infrastructure (PKI) supports the distribution and identification of public encryption keys, enabling users and computers to both securely exchange data over networks and verify the identity of the other party. Within that infrastructure, a trusted party called a certificate authority (CA), acts as the root of trust and provides certificates that authenticate the identity of individuals, computers, and other entities. If one CA is compromised, the security of the entire PKI is at risk. Hackers could intercept sensitive communications between users or at a minimum cause some business interruption as companies must get new trusted certificates.

The following exhibits display the Client's loss potential from three deterministic aggregation scenarios.



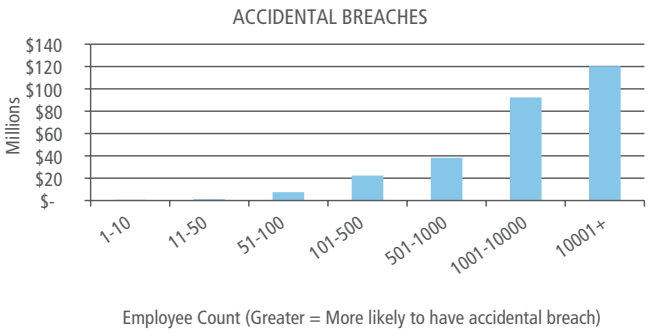
CLOUD BREACH

A major cloud provider experiences a breach and goes down for five days. Companies doing business with the provider are unable to access their data and, as a result, experience a business interruption loss.



PAYMENT PROCESSOR BREACH

A major payment processor experiences a breach and goes down for five days. Companies who rely on the vendor for purchase payments experience a business interruption loss.



AGGREGATION OF ACCIDENTAL BREACHES

A malicious virus that causes servers to crash is distributed to millions via email. Thousands of companies experience simultaneous breaches as unwary employees open their emails.

(cont. from page 3)

Verisk Analytics and AIR have created the industry's first global cyber exposure data standard. The Verisk Cyber Exposure Data Standard, along with the AIR Preparer's Guide, can help companies understand their exposure and aggregation risk, evaluate that risk, and make underwriting or pricing decisions today.

The standard was designed to be open and flexible, which allows re/insurers to begin implementing it with the data they have available now and grow into populating new data fields over time as the understanding of cyber risk evolves or resources permit.

Any organization can be entered into the standard, regardless of whether it has explicit cyber coverage or not, including companies, governmental organizations, non-governmental organizations, non-profits, and others. The preparer's guide provides details about the various fields, including ones labeled "Common Core," which—after consulting with Lloyd's of London—were deemed especially important to collect.

To make the standard and preparer's guide truly practical and immediately ready to use within your organization, AIR has made available an SQL schema ready for download and implementation.

Perform Deterministic Analyses Now

Implementing the Verisk Cyber Exposure Data Standard within your risk management process puts your organization in a position to begin modeling your cyber risk immediately. The comprehensive and flexible nature of our standard provides you with the ability to perform deterministic analyses of virtually any cyber event you can imagine. The insights you gain from these deterministic analyses can then be used to make decisions about managing the cyber risk within any portfolio.

To supplement the unlimited number and variety of cyber scenarios you can begin modeling, AIR is also releasing a unique cyber scenario each month. The AIR Open Source Cyber Scenarios will serve as practical examples of how the schema can be used to perform deterministic scenario modeling of an insurer's book of business. AIR's scenarios will include a detailed description of a potential cyber event and be accompanied by SQL scripts that capture that event's severity and loss potential. These SQL scripts are based on the open source Verisk Cyber Exposure Data Standard, enabling you to view all the assumptions made within the scenario and modify them according to your view of risk.

About the Upcoming AIR Probabilistic Cyber Risk Model

AIR Worldwide's forthcoming probabilistic cyber risk model will help insurers and reinsurers manage accumulations of cyber risk as well as assess and evaluate the risk of individual contracts. The probabilistic model follows the same modeling framework and generates the same output as traditional natural catastrophe models. AIR's cyber model will be differentiated not only by the expertise of the scientists who are building it, but also by the unique data sources that underlie the model's assumptions.

The hazard component of the AIR Cyber Model defines the frequency and severity of the cyber events being modeled, and it is informed by an extensive data set of historical breaches. AIR has partnered with Risk Based Security and is using their data to build distributions of the number and type of cyber events per year, the industries targeted, and the revenue source affected. These distributions are then leveraged to create a stochastic catalog of 100,000 simulated years of cyber events. This event catalog is a representation of what could happen next year and can be used to define the probability of a specific cyber event occurring.

The vulnerability component defines the damage that can result from a cyber loss event, helping inform re/insurers of the relative riskiness of individual companies and the industries they operate in. An exclusive partnership with BitSight gives AIR access to vulnerability data that is updated daily, giving re/insurers the ability to obtain a real-time view of their exposure's cyber risk.

The AIR Cyber Model will use the financial module within Touchstone®, which means you can expect losses to be delivered in the same perspectives—average annual loss (AAL), exceedance probability curves, and secondary uncertainty curves, etc.—for both single contracts or large portfolios. This will allow losses to be applied to endorsements, global coverages, and sublimits, ultimately defining the financial loss that a re/insurer can expect after a cyber event.

AIR has already reached agreements with many re/insurers to obtain exposure and claims data for model calibration and validation, with more expected. In addition, AIR's relationship with companies in the Verisk Analytics family, such as Argus™, ISO, and Verisk Maplecroft, provide other sources of cyber insights that no other modeler can obtain. For these reasons, AIR is in a position to uniquely transform your exposure data into a comprehensive view of cyber risk.

To learn more, please contact your AIR representative or visit us at:
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 (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.

AIR
A Verisk Business