Cyber insurers have mostly relied on limited data or broad assumptions to inform their risk management decisions. As a result, insurers can struggle to determine the largest losses that can be expected and how likely these are to occur. The AIR Probabilistic Cyber Model provides insights to help (re)insurers manage the risk from security breach incidents (including phishing/social engineering scams, malware and other computer hacks, accidental issues, and unauthorized data disclosures), as well as business interruption incidents (cloud service downtime), which continue to cause the majority of cyber insurance claims.
The profitability and growth potential of cyber insurance is attracting more (re)insurers to the market, and because of increased competition, pricing is set by supply-and-demand dynamics rather than risk-based assessments. Any insurer’s worst nightmare is experiencing a major loss event that puts the viability of the business in jeopardy. To avoid being labeled as “naïve capital” in this market, insurers must understand how deep in the red their business could become and how they can select the best risks to continue growing while maintaining their overall profitability.

The AIR Probabilistic Cyber Model helps insurers understand their loss potential to both attritional and extreme events before they occur. This data-driven model leverages machine learning and stochastic simulations to deliver insights about the likelihood of cyber incidents and the financial impact that those incidents could have on individual risks or books of business. Furthermore, the model enables insurers to keep up with the evolving cyber risk landscape because it has been built with a transparent and flexible modeling framework that allows analysts to study the drivers of modeled loss and test their own views of risk.

**Robust Incident Loss Database Informs View of Risk**

AIR has created an incident loss database comprising data on more than 77,000 cyber incidents, such as lost devices, social engineering scams, computer hacks, unauthorized data disclosures, and cloud service downtime. Loss incident data is obtained by monitoring and curating information from sources that include government information releases, media alerts, judicial sources, and data security reports. These sources only offer a partial view of all cyber incidents, however,
because most incidents that get reported are the ones that larger organizations experience, as the media typically do not report incidents that occur at small to mid-sized organizations. In addition, AIR has obtained claims data from several cyber insurers to further validate its view of risk. To compensate for biases due to underreporting, AIR calibrates the model's view on frequency by incorporating insurance claims data from several cyber insurers. This calibration is especially important when accounting for the risk to small-to mid-sized businesses.

Cyber Industry Exposure Database Provides Global View of Risk
AIR has also created a comprehensive industry exposure database that underlies the probabilistic cyber model. This database represents the insurable global cyber market and contains firmographic and technographic information for more than 12 million organizations that can be used to augment your exposure data. When company-specific detailed data isn’t available, the model can provide aggregated detailed data and produce industry- and region-specific market shares that can be applied to organizations in the United States, Canada, United Kingdom, Europe, Japan, Australia, and rest of world (RoW). Insurers can leverage this database to begin modeling cyber risk with as little information as the name of the organization name or the organization’s industry and revenue.

Machine Learning Identifies Likelihood of Loss
There are many drivers of cyber risk, but which ones are truly predictors of loss and which ones should underwriters be collecting data on? To determine the likelihood of an organization experiencing a security breach and the factors that drive risk, AIR leveraged machine learning techniques best suited to identify signals in the data that other modeling approaches would likely miss. This machine learning-driven approach was trained using our incident loss and global cyber exposure databases.

The frequency difference between public and insurance claims data reveals that there is an underreporting bias in publicly reported data, in particular for small- to mid-sized businesses.

An organization’s revenue and industry provide enough information to determine the probability of breach, but additional rating variables can be used by the model to further differentiate the risk. AIR has identified several technographic features related to an organization’s security policies, level of malware, and filesharing activity that have a meaningful impact on the probability of breach; these features are used as inputs to the probabilistic model. Insurers can focus on collecting information on these attributes at the point of underwriting or rely on ARC’s industry exposure database to backfill their data.

Optimize Underwriting of Attritional Cyber Security Breaches
Security breaches are the most frequent type of cyber incidents, yet insurers often resort to limiting their exposure when the risk is not well understood. The AIR Probabilistic Cyber Model provides insurers with the insights they need to overcome this challenge so that security breach risks can be underwritten more effectively. With pricing determined by supply-and-demand dynamics, insurers can leverage the model’s ability to differentiate risk to improve their risk selection and ensure that the most viable risks are underwritten. In addition, insurers can identify opportunities to grow premiums by testing their current underwriting guidelines against notional terms and conditions that permit the insurer to take on additional risk but stay within their predefined risk appetites. Different waiting periods, attachment points, and limits can be tested using the model.
The widespread adoption of cloud services has made providers of these services a major source of systemic risk that could cost the global economy billions in business interruption losses if a major downtime incident were to occur. Given that each cloud service provider in the market is a uniquely architected and independently managed business, insurers must go beyond simply tracking limits associated with each provider to understand the losses that can be expected from each. To meet this need, the model uses stochastic modeling techniques to simulate downtime events for more than 100 different cloud service providers. Each unique event describes which cloud provider went down, the cause of the downtime, downtime length and how many of the cloud provider’s data centers were affected. The AIR Probabilistic Cyber Model makes it straightforward to quantify how some cloud providers are riskier than others and how systemic incidents can impact an insurance portfolio.

To truly own the risk, cyber insurers must keep up with the rapidly evolving risk landscape and be able to confidently justify their decisions to stakeholders. Whether it be by changing their view of risk based on newly discovered vulnerabilities or adjusting underwriting strategies to differentiate their products, transparent and flexible analytics can help you make informed decisions on how to continuously evolve the cyber line of business.

The AIR Probabilistic Cyber Model differentiates the tail risk associated with the downtimes of specific cloud service providers, such as Microsoft, Amazon, Google, and others.

The European Union’s General Data Protection Regulation (GDPR) came into effect in mid 2018. The implications of GDPR for organizations conducting business in Europe that experience a data breach are that they are now subject to paying a maximum fine of 20 million euros or 4% of global annual revenue (turnover), whichever is higher. The latest release of ARC provides users with optional functionality to include potential fines as part of the probabilistic model output due to the security breach cause of loss.

The AIR Probabilistic Cyber Model offers transparency into its assumptions by exposing the underlying metadata that drives losses, including the complete catalog of simulated events, the technographic data used to differentiate risks (such as common cloud service providers associated with a specific company), and the industry-specific vulnerability factors (i.e., parameters that determine how much of a company’s revenue depends on the cloud). For even more flexibility, the model enables users to test unique views of risk and their impact on expected losses by allowing users to adjust the industry-specific vulnerability factors, and modify the event catalog data to adjust the frequency of cybersecurity incidents.
Model at a Glance

<table>
<thead>
<tr>
<th>Modeled Incidents</th>
<th>Uncorrelated security breaches, which include lost devices, hacking and malware infections, skimming, social engineering, accidental issues, and unauthorized data disclosures</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Cloud service provider downtime</td>
</tr>
<tr>
<td>Model Domain</td>
<td>Global</td>
</tr>
<tr>
<td>Catalog Size</td>
<td>50,000 years</td>
</tr>
<tr>
<td>Supported Insurance Coverages</td>
<td>Security Breach Expense and Business Interruption Expense</td>
</tr>
<tr>
<td>Industry Exposure Database</td>
<td>More than 12 million organizations globally</td>
</tr>
<tr>
<td></td>
<td>Company-specific technographic data for more than 100,000 companies</td>
</tr>
<tr>
<td></td>
<td>Region-specific industry market share data for U.S., Canada, Great Britain, Europe, Japan, Australia, and rest of world (RoW)</td>
</tr>
<tr>
<td>Model Output</td>
<td>AAL, Exceedance probability losses and the underlying metadata for each incident type</td>
</tr>
<tr>
<td></td>
<td>Exposure data on technographic attributes of modeled organizations, such as cloud provider usage</td>
</tr>
</tbody>
</table>

Model Highlights

- AIR leveraged data on more than 77,000 cyber incidents from public and insurance sources to develop its view of risk
- Underlying the probabilistic model is a global exposure database that can be used to augment exposure data
- Machine learning techniques were used to determine incident frequency and the factors that affect the likelihood of incidents occurring
- Underwriting strategies can be improved by using model output to identify the most viable risks and the optimal level of insurance coverage
- Insurers can improve their diversification strategy by differentiating the accumulations of risk within portfolios using granular technographic data
- The model was developed with a transparent and flexible framework that allows users access to the underlying assumptions and the ability to create different views of risk

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 incidents. Insurance, reinsurance, financial, corporate, and government clients rely on AIR’s advanced science, software, and consulting services for catastrophe risk management, insurance-linked securities, longevity modeling, 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.