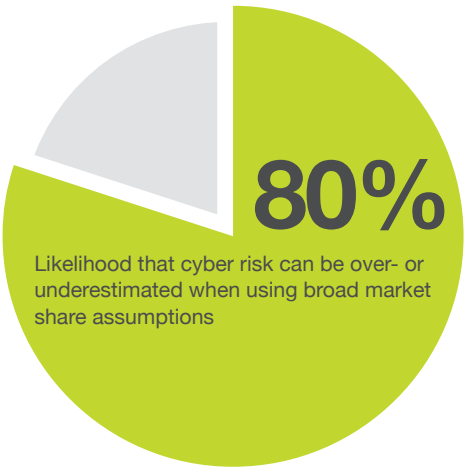
ARC: A New Era of Cyber Resilience

Highlights

ARC (Analytics of Risk from Cyber) reveals critical insights by giving underwriters and risk managers the ability to:

- Evaluate any commercial policy, including those vulnerable to silent cyber
- Measure and monitor aggregations of cyber risk within a portfolio
- Estimate potential insured cyber losses for individual companies or portfolios

The cyber insurance market is complicated by a lack of standardization and high degrees of uncertainty. In fact, the biggest obstacle to growing a cyber line of business today is a lack of understanding of the exposures. Traditional actuarial methods for estimating risk aren't sufficient. However, that's not discouraging new entrants to the market, which is becoming increasingly competitive. This increased competition, in turn, can discourage underwriters from pushing for more information from potential insureds out of fear that they will seek coverage elsewhere. This shortage of data propagates up to the enterprise risk management level where uncertainty about a portfolio's risk aggregation can prevent managers from taking on more risk.



As a result, insurers tend to rely on little more than intuition or broad industry assumptions that may not be appropriate for their own strategy and risk appetite. With corporate boards and regulators concerned about the solvency of organizations, the possibility of mismanaging this risk cannot be taken lightly.

At the same time, cyber risk is transitioning from an emerging threat to a promising business opportunity. A cyber line of business can bring new profits as the cyber insurance market is expected to triple over the next several years, benefiting new and experienced cyber insurers alike.

AIR

AIR's Detailed Accumulation Approach to Managing Cyber Risk

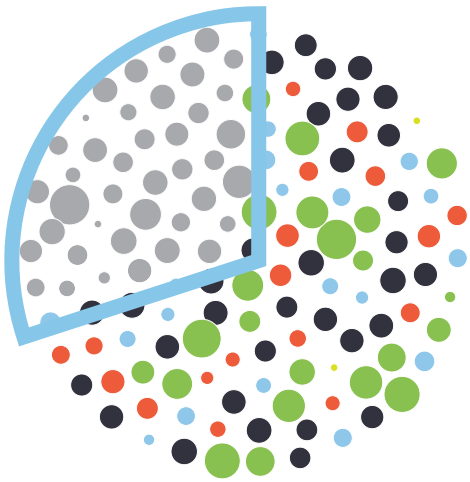
Given that cyber risk can be found within virtually any policy that doesn't explicitly exclude it— including Directors & Officers (D&O), Errors and Omissions (E&O), general liability, and others —the potential for losses across many lines of business can put the profitability of an entire portfolio in danger. (Re)insurers need tools to accurately measure and monitor the impact of cyber threats that can trigger simultaneous financial losses across multiple organizations. Sources of aggregated risk that can cause such events include the widespread use of commercial software with unknown or unpatched security vulnerabilities, reliance on third-party organizations for services critical to business operations, or the use of shared infrastructure.

AIR developed a detailed accumulation approach as an improvement over existing methods that rely on market share data, as it removes much of the uncertainty that can exist when industry averages are used to determine which companies would be impacted when performing a scenario analysis. Market share approaches can provide broad approximations when little detailed data about a portfolio is available, but it is likely to either over- or underestimate the risk, possibly significantly, for specific portfolios.

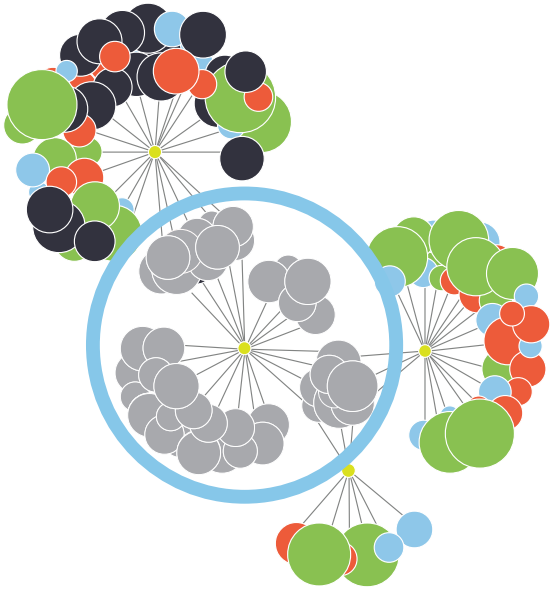
ARC's detailed accumulation approach utilizes data about a company's sources of aggregated risk to determine with greater certainty which companies would be impacted by the aggregation scenario. AIR's approach provides a more confident view of the risk because it identifies the exposures that would actually be affected by the event and omits those that should not be considered.

Proprietary Database of Industry Exposures Enhances View of Cyber Risk

Cyber insurers are well aware of the importance of gathering detailed exposure data at the point of underwriting, particularly now, as new modeling technologies are coming online. But sometimes market conditions can discourage the collection of detailed data, which is why ARC includes a proprietary database of industry exposures that users can leverage to enhance their view of the risk.



Market Share Approach



Detailed Accumulation Approach

Two identical portfolios are tested against the same cloud failure cyber scenario. Using a market share approach (left) the exposures impacted by the scenario are arbitrarily carved out. For example, if Cloud Vendor X has a 30% market share, then you would assume that same share exists within your portfolio and that 30% of your insureds would be at risk of experiencing a loss if that cloud provider were to go down. With ARC's detailed accumulation approach (right), exposures are organized around the specific cloud providers each company actually relies on. By identifying these aggregation points, only the exposures known to be at risk are considered.

AIR has combined data from multiple commercial and public sources to develop a comprehensive view of the insurable cyber market in the United States and key companies across the world. AIR's detailed industry exposures contain information about a company's demographic, information technology, and cybersecurity profile as outlined by the Verisk Cyber Exposure Data Standard. For millions of organizations, AIR has data on risk attributes such as company industry and size, data storage and transfer mechanisms, antivirus effectiveness, and cloud service provider.

Insurers' own data will always be prioritized, but AIR provides advanced algorithms that cross-reference and match the industry exposures with the individual organizations in the portfolios that are being analyzed. When an insured company's name is available, a host of additional cyber risk–related information can be augmented; but even portfolios with only data on industry and revenue can benefit from the augmentation of average characteristics from the industry exposures.

Evaluate any Commercial Policy

To estimate expected losses from cyber incidents, AIR employs a ground-up methodology that first considers an organization's risk profile as the basis for determining the magnitude and cause of loss. As a result, users have the flexibility to determine how each cause of loss, such as security breach expense or business interruption, is best represented within the insurer's unique policy coverage framework.

Any commercial policy can be evaluated by ARC:

Standalone Cyber

Policies that solely cover damage resulting from cyber security incidents

Cyber Endorsements

Supplemental cyber coverage added to existing commercial policies, such as D&O, E&O, general liability, or property

Silent Cyber

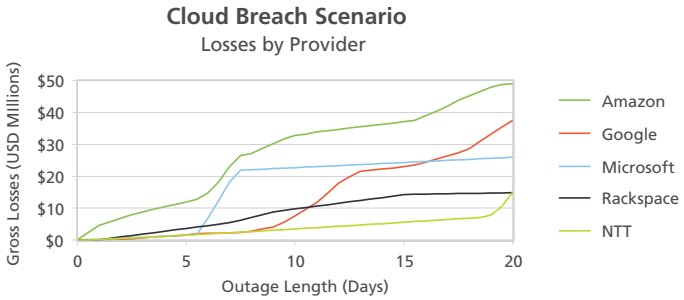
Any policy that doesn't explicitly include or exclude cyber

Model Cyber Scenarios

Scenario modeling has become integral to supporting key decision-making processes, such as accumulation management, the development of underwriting guidelines, and reinsurance purchasing. The evolving nature of cyber risk and the variety of risk management strategies available means each insurer must define the cyber scenarios that are most relevant to them. ARC gives you the flexibility to do just that. AIR's cyber scenarios are used to estimate the financial impact of a defined event on an individual company or portfolio. Over a dozen scenarios are available and, with the ability to modify the severity parameters, risk managers can implement their own view of the risk, test the sensitivity of portfolios to different event circumstances, and explore the impact of adjusting cyber policy terms.

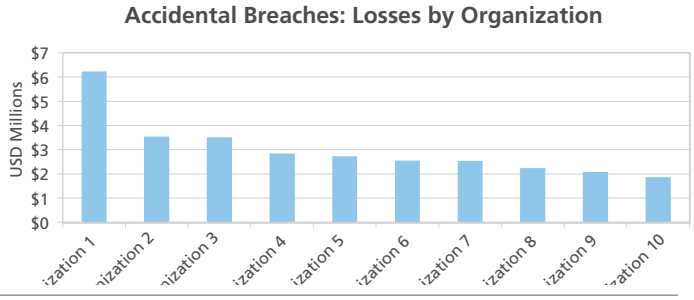
BUSINESS INTERRUPTION SCENARIOS

Losses occur when there is a failure of service from a third-party IT provider, such as cloud, payment processor, domain name system, online advertisement, or mail exchange. During the downtime, a company may lack access to data critical for running its business or its revenue channel may be closed, either of which could result in a (contingent) business interruption claim.



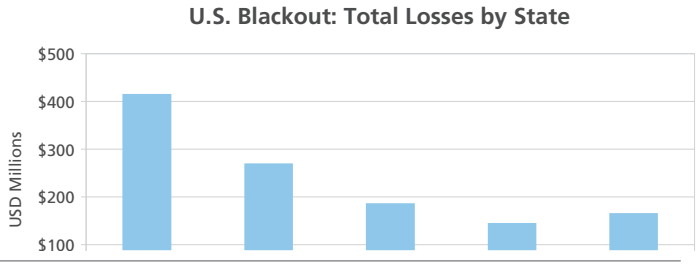
SECURITY BREACH SCENARIOS

Security breaches occur when confidential data is made available to the public. As a result, a breached company can make an insurance claim to cover its own recovery expenses or defend against lawsuits. AIR's current security breach scenario considers breaches caused by employees who accidentally cause data to be stolen or lost.



BLACKOUT SCENARIOS

A cyber attack on the electric grid has the potential to impact both commercial and personal lines of business. The broad range of causes of loss—from liability to business interruption and physical damage—means that the threat of silent cyber looms largest in these scenarios. In addition to developing its own cyber blackout scenarios, AIR has modeled the Lloyd's blackout scenarios for the U.S. and UK.



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.

To learn more, please contact your AIR representative or visit us at: air-worldwide.com

AIR
A Verisk Business