Munich RE

Protection against cyber breaches

Recent headlines about data breaches and ransomware attacks have led to increased scrutiny by many organizations about their preparedness for these events. Companies are looking for ways to mitigate risk, primarily through cyber insurance.

Munich Reinsurance America, Inc. supports cyber insurance initiatives in multiple ways, ranging from facultative reinsurance for high-hazard single-risk programs, to treaty reinsurance for clients with mature cyber capabilities, to client-tailored, turnkey cyber products for small to mid-sized entities. Some clients may be capable of retaining some of the risk associated with cyber insurance but may lack the expertise and resources that must accompany cyber insurance products. Munich Re offers a variety of solutions.

Growing exposures

Gemalto's Breach Level Index showed that 2.6 billion records were stolen, lost or exposed globally in 2017, up by 88% from 2016.[1] Over the past five years, nearly 10 billion records have been lost, stolen or exposed, with an average of five million records compromised every day.

And data breaches continue to happen daily, in too many places at once to keep count. Most organizations confirm they have now suffered at least one cyber incident, but they may not realize these incidents' full impact. A Deloitte study shows that "hidden" costs can amount to 90 percent of the total business impact on an organization and will most likely be experienced two years or more after the event.[2]

As businesses and consumers become more aware of the risks associated with cyber attacks through internet use, demand for cyber insurance increases.

Turnkey product overview

For the sophisticated 21st century P&C insurer ready to embrace this new insurance vertical, Munich Re's innovative turnkey product offering rethinks cyber insurance products by providing full product support, including:

- Risk transfer (up to 95% QS Treaty reinsurance capacity; limits up to $15m)
- Underwriting guidelines
- Cyber product training (underwriting and claims)
- A private-labeled risk management portal (provides cyber news, incident roadmaps, risk management tools, white papers, webinars, training tools and access to industry experts, including consultation with a Breach Coach)
- Post-Breach Services Panel (includes firms specializing in IT forensics, regulatory compliance, call center services, public relations and breach response services)
- Claims Third Party Administrator

Targeted insureds and underwriting eligibility

- Most small to medium-sized enterprises (SME), up to $250 million in revenue, are eligible. Select insureds in high-risk classes are ineligible, such as adult entertainment, social media providers and trading exchanges.
- Most classes of business are subject to risk-responsive, individual underwriting
- Most SME businesses that are eligible require standalone cyber coverage (e.g., health-care providers, retailers, restaurants, construction, architects, engineers, lawyers, accountants and non-profits)

Limits

Average limits of $1 million to $5 million; maximum of $15 million on eligible policies

Exposures and loss scenarios

Covered losses may include:

- Website publishing liability—third party liability coverage for loss and defense expenses arising out of intellectual property infringement and personal injury perils that result from an error, misstatement or misleading statement on the insured's website
- Security breach liability—third party liability coverage for loss and defense expenses arising out of a security breach or arising out of the transmission of a virus to a third party
- Regulatory proceedings—coverage for loss and defense expenses, including fines and penalties if insurable by law, incurred from a regulatory proceeding resulting from a covered security breach
- Programming/technology E&O liability—third party liability coverage for loss and expenses arising out of a programming error or omission
- Replacement or restoration of electronic data—costs incurred by the insured to replace or restore electronic data or computer programs
- Extortion threats—expenses, including ransom payments, resulting from an extortion threat made against an insured
- Business income and extra expense—costs of a public relations firm to respond to negative publicity resulting from a cyber incident or security breach

- Security breach expenses—costs incurred resulting from, and in response to, a security breach, including forensic investigations, legal counsel and call center services. Also includes costs of notifying consumers and providing credit/identity-monitoring services as required by various state, federal or international laws or regulations.

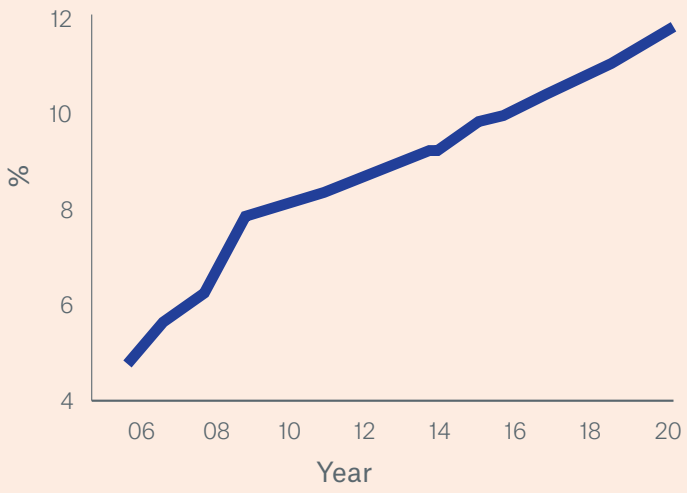
Client benefits

With our cyber toolkit, we're offering primary insurers the necessary tools to enter a new market by providing technical expertise, reinsurance capacity and such important tools as a risk management portal and access to post-breach third party service providers.

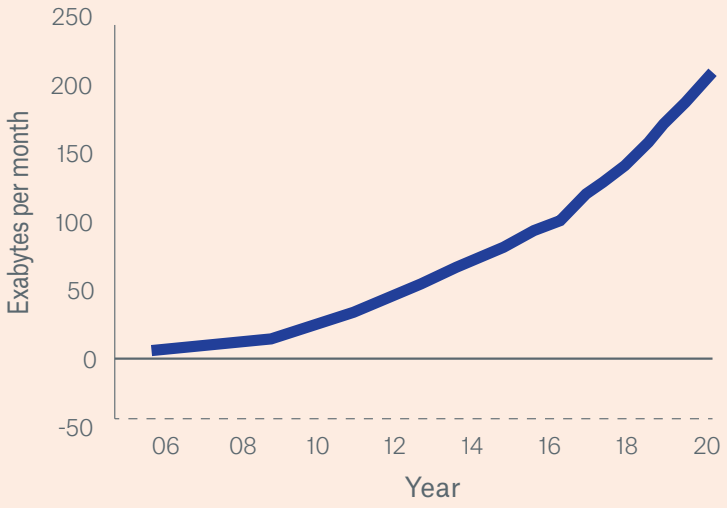
How is our cyber offering different?

- Munich Re's cyber offering is unique because our goal is to support clients who want to enter the cyber market now but have the goal of expanding their internal cyber capability and expertise over time
- We are the only reinsurer in the market with full flexibility to support an industry standardized product and a willingness to support our client's proprietary cyber product
- Unlike other reinsurers, we don't require our clients to offer a reinsurer-mandated cyber product and limit you from participating in the risk. Our flexibility enables our clients to grow into the business and differentiate themselves.

Percentage of services conducted online



Internet traffic volume



Source: www.IBISworld.com

Cyber by the numbers

5th
Rank of cyber in terms of "most important risk" to U.S. firms[4]

2.6b
Number of records stolen, lost or exposed in 2017[1]

72%
Percentage of cyber attacks that occurred in SMEs[3]

$349k
Average cost of a breach in 2017[6]

41%
Percentage of cyber losses stemming from a malicious breach[2]

$4.1b
Projected size of the standalone U.S. commercial cyber liability market by 2020[5]

Sources

1. https://blog.gemalto.com/security/2018/04/13/data-breach-stats-for-2017-full-year-results-are-in/, April 2018
2. https://www.advisenltd.com/wp-content/uploads/2017/04/2018-advisen-cyber-guide.pdf
3. "IBISWorld Industry Report: Cyber Liability in the US", May 2016
4. AON Inpoint: "Global Cyber Market Overview", June 2017
5. Verisk: "Sizing the Standalone Commercial Cyber Insurance Market", February 2018
6. https://netdiligence.com/wp-content/uploads/2017/11/NetDiligence_2017CyberClaimsStudy_Infographic_v1.1.pdf, April 2018

Product and services provided by Munich Reinsurance America, Inc. ("Munich Re") and its affiliates.

Any descriptions of coverage contained in this brochure are meant to be general in nature and do not include nor are intended to include all of the actual terms, benefits and limitations found in an insurance policy. The insurance policy and not this brochure will form the contract between the insured and insurance company, and governs in all cases. This brochure is for information purposes only and is not intended to be legal, underwriting, financial or any other type of professional advice and the recipient should consult with its own advisors with respect to the information contained herein and its applicability to the recipient's particular circumstances.