Cyber crime is increasing – **make sure your business is protected**

NOT IF, BUT HOW

Munich RE

Data breaches, ransomware attacks, and other cyber crimes are on the rise. They can cause extensive business disruption, damage a company's reputation, and even force a business to shut its doors. Almost 50% of small businesses have already experienced a cyber attack.[1]

Munich Re US, 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

In the last eight years, over 9.7 billion data records have been lost or stolen. Over 7 million data records are compromised every day. Cybercrime, including ransomware, is growing exponentially, affecting businesses of all sizes.[2]

Cyber attacks cost companies $200,000 on average and can put many companies out of business.[3] Hidden costs can be as harmful as direct costs, including business disruption, reputational risk, downtime, and lost opportunities.[4] Downtime costs, due to ransomware attacks alone, averaged $283,000.[5]

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 (meaningful capacity for limits up to $10M)
- Underwriting guidelines
- Cyber product training (underwriting and claims)
- Best Practices for Risk Assessment
- 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)

Limits

Average limits of $1 million to $3 million; maximum of $10 million on eligible policies.

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 stand-alone cyber coverage (e.g., retailers, restaurants, construction, architects, engineers, lawyers, accountants, and non-profits)

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
- 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 impacted consumers and providing credit/identity-monitoring services as required by various state, federal, or international laws or regulations.

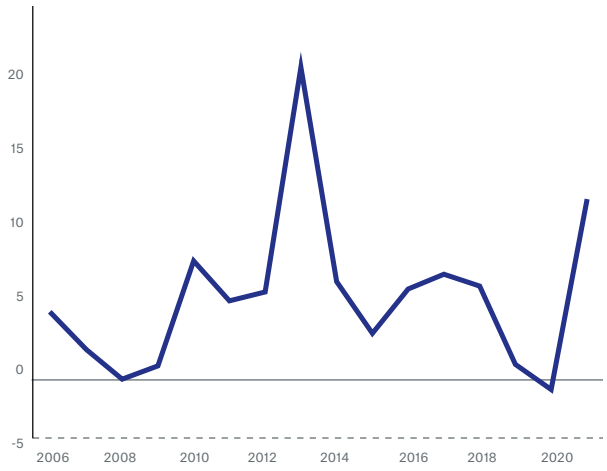
Client benefits

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.

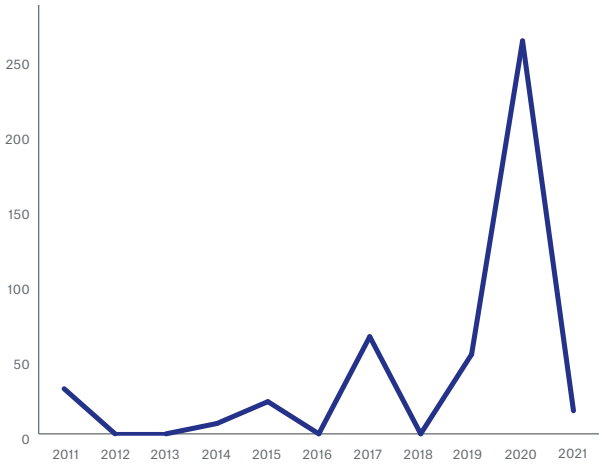
How is our cyber offering different?

- 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 offer our clients the full flexibility to support an industry standardized product and a willingness to support our clients' 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: IBISworld.com

Cyber by the numbers

#1 Business risk: cyber incidents[6]	**36B** Breaches involving small businesses 2020[7]	**$435K** Average business interruption cost SMEs[8]
$192K Average recovery expense SMEs[8]	**68%** Business leaders feel cyber risk increasing[9]	**72%** Increase in cyber crime last 5 years[9]

Sources

1. https://www.solvereone.com/pages/cyber-attacks-on-small-businesses-increasing-in-2021/
2. https://blogvaronis2.wpengine.com/the-world-in-data-breaches/
3. https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html
4. https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf
5. https://www.munichre.com/topics-online/en/digitalisation/cyber/cyber-insurance-risks-and-trends-2021.html
6. https://www.cfo.com/risk-management/2020/01/cyber-incidents-ranked-as-no-1-business-risk/
7. https://www.verizon.com/business/resources/reports/dbir/
8. https://netdiligence.com/wp-content/uploads/2021/03/NetD_2020_Claims_Study_1.2.pdf
9. https://www.accenture.com/_acnmedia/PDF-96/Accenture-2019-Cost-of-Cybercrime-Study-Final.pdf#zoom=50

Printed July 2021