

Cyber: Physical Damage Insurance



Cyberattacks can cause physical damage, including fire, explosions, and other effects usually covered by property programs. Cyberattacks or failures can also cause disruptions in process controls or communication components of critical infrastructure such as water pumps, pipeline valves and industrial environments (e.g., SCADA). These events can impact safety and security functions in building controls, such as forcing an autonomous vehicle off the road. The Lloyd's 2022 report, "Shifting powers: physical cyber risk in a changing geopolitical landscape," provides several scenarios detailing physical cyber risk that has already caused damage in the real world¹.

Cyber insurance typically excludes physical and property damage, and property and casualty insurance have often amended their policies to limit coverage for types of physical damage caused by cyber events. Insurance purchasers can review their programs to ascertain if there are gaps and understand their exposures to uninsured cyber-caused physical loss. For those with coverage gaps, the insurance markets have created a stand-alone solution.

Carriers have created facilities blending property and cyber market coverages to fill gaps created by cyber exclusions on property and cyber policies. The main three options include the following:

- Cyber insurance policies with an affirmative Property Damage DIC endorsement
- Standalone Cyber Property Damage policies
- Cyber insurance with affirmative non-physical and physical coverages

Up to \$250M is available on a standalone basis or combined with traditional cyber insurance coverage. Further limits are available where markets are added on an excess basis but usually include up to \$300M of coverage.

Required Information

Insurers can provide a non-binding indication with reduced information, which would include the following:

- Insured's cyber submission
- Annual revenue or turnover
- Business interruption values
- Insured's property policy

Underwriters will require an additional Operational Technology or Cyber Property Damage application or a broad-ranging underwriting call with the customer to provide a bindable quotation.

Physical impacts that might be covered by such a program will vary depending on the insured's industry, type of business, use of technology, IT controls and ownership and control of physical assets.



How We Can Help

The Brown & Brown team has been tracking developments and can provide advice on emerging gaps and exposures. Our cyber risk models can provide scenarios to evaluate individual exposures and identify gaps in insurance programs. Please contact your Brown & Brown representative to further understand our capabilities.

**FOR FURTHER INFORMATION
PLEASE CONTACT**

1. https://assets.lloyds.com/media/0926f9be-0f3d-49cc-9960-52accc888aad/Lloyds_Shifting_%20Powers_Physical_%20Cyber_Risk_Final_2906.pdf



How Brown & Brown Can Help

Connect with our Brown & Brown team to learn about our knowledge in your industry, how we build our risk mitigation strategies and how we can aid your business in building a cost-saving program.



Find Your Solution at [BBrown.com](https://www.BBrown.com)

Brown & Brown, Inc. and all its affiliates, do not provide legal, regulatory or tax guidance, or advice. If legal advice counsel or representation is needed, the services of a legal professional should be sought. The information in this document is intended to provide a general overview of the topics and services contained herein. Brown & Brown, Inc. and all its affiliates, make no representation or warranty as to the accuracy or completeness of the document and undertakes no obligation to update or revise the document based upon new information or future changes.

©2024 Brown & Brown. All rights reserved.