CONTACT US

Dave Perkins, RPLU
(508) 848-4263
dave.perkins@igpspecialty.com

Bricking Coverage Explained

Bricking coverage in cyber insurance covers the costs to replace electronic devices, such as computers and smartphones, that are rendered unusable and beyond repair due to a cyberattack. This coverage helps businesses replace essential hardware damaged by malware or other cyber incidents, which can otherwise cause significant system downtime and financial losses.

It is important to review the specific terms and limitations of bricking coverage in your policy with a broker, as coverage can vary significantly between different insurers and policies.

What is Bricking?

Bricking occurs when malicious software (malware) wipes or corrupts a device's operating system or firmware, making the hardware inoperable and unrecoverable.

What Bricking Coverage Pays For

This coverage provides financial assistance to replace damaged hardware.

Examples of Devices Covered

Policies can cover computers, smartphones, tablets, and other essential electronic devices that are bricked by a cyberattack.

Key Considerations for Bricking Coverage

Policy Variations

The specific terms and conditions, including the scope of coverage and any limits, can differ greatly between policies.

Physical vs. Digital Damage

Bricking coverage typically applies to actual damage to the hardware, not just digital issues like encrypted files or a corrupted operating system that might be recoverable.

Associated Costs

While policies might cover the cost of the replacement hardware itself, they may not cover all related costs, such as the expense of installing the new equipment or business interruption losses.

Broader Cyber Insurance

Bricking coverage is a component of a larger cyber insurance policy and should be discussed with your broker to ensure comprehensive protection.

©2026 Innovation Growth Partners Specialty, LLC | igpspecialty.com