COVERAGE INSIGHTS

BRICKING COVERAGE IN CYBER INSURANCE

Bricking is a type of cyberattack that renders a device unusable, effectively making it a "brick." It targets hardware—disabling computers, tablets, hard drives, phones and other technological instruments. Unlike typical cyber incidents involving data theft or software disruption, bricking corrupts essential software or firmware, leaving the device permanently inoperable, even if the physical components themselves are not visibly damaged. While data loss can often be restored and software issues patched, bricking can lead to irreversible hardware failure and extended downtime.

As destructive bricking attacks become more common, businesses should mitigate their risks by ensuring their cyber insurance policies cover these types of events. This article provides more information on bricking coverage, including what it is and what it typically includes. It also discusses the common limitations and coverage gaps of base cyber and property insurance policies and provides an overview of best practices for insurance buyers.

WHAT IS BRICKING COVERAGE?

Bricking coverage is a specialized enhancement within a cyber insurance policy designed to cover the costs of replacing or restoring devices that have been rendered inoperable due to a cyberattack. These expenses can be significant depending on the scale of the incident.

Standard cyber and property insurance policies may exclude coverage for cyber-caused hardware failures, especially when there is no physical damage in the traditional sense. This creates a coverage gap that bricking endorsements are specifically designed to fill. As cyber threats evolve, it's increasingly crucial for organizations to review their cyber and property insurance policies to determine whether bricking coverage is included or must be added separately. Not all insurers automatically include bricking coverage, so it must be purchased as an add-on endorsement in many cases. Ensuring this protection is in place can be critical to minimizing operational disruption and financial loss following a bricking cyberattack.

WHAT DOES BRICKING COVERAGE TYPICALLY INCLUDE?

Bricking coverage generally includes the cost of replacing hardware that has been rendered inoperable by a cyberattack. This can involve a wide range of devices, including laptops, point-of-sale terminals, servers, and Internet of Things (IoT) equipment that are essential to business operations. Coverage usually applies only when devices cannot be repaired or restored, meaning insureds must demonstrate permanent inoperability. When these devices are "bricked," they often cannot be repaired or restored through software fixes, making full replacement necessary.

In addition to the hardware itself, bricking coverage may also provide expenses related to the replacement process. This can include the cost of installation, labor for swapping out devices, and proper disposal of the damaged equipment. While specifics vary, bricking coverage can significantly reduce the financial and operational burden on an organization following a bricking attack.

COMMON POLICY LIMITATIONS AND COVERAGE GAPS

Cyber and property insurance policies often contain limitations and coverage gaps that can significantly impact recovery following a bricking incident. As this type of loss may be excluded from base policies, an endorsement may be needed to receive coverage.

Even when bricking is covered, exclusions may apply, such as limiting coverage to certain types of attacks.

COVERAGE INSIGHTS

BRICKING COVERAGE IN CYBER INSURANCE

Additionally, sub-limits, waiting periods and other exclusions within the policy (e.g., excluding the cost of installing the replacement equipment) can result in out-of-pocket expenses, reducing its overall effectiveness. Some policies only cover mass bricking events (e.g., affecting multiple devices), while others apply coverage on a per-device basis, which can affect claim outcomes.

BEST PRACTICES FOR INSURANCE BUYERS

To secure protection against bricking-related losses, insurance buyers should follow these best practices when evaluating and negotiating coverage:

+ **Review cyber and property insurance in tandem**—Thoroughly evaluate these policies together to identify and address potential coverage gaps. Pay particular attention to how each policy addresses bricking while verifying whether it's covered, the coverage limits, and what specific events or triggers activate that coverage.

+ **Identify high-risk devices that could require bricking protection**—Conduct an inventory of critical hardware assets, especially those that are essential to operations or difficult to replace. Some devices (e.g., servers, industrial control systems, and specialized medical or manufacturing equipment) may warrant additional bricking coverage due to their importance, vulnerability and replacement cost.

+ **Engage with brokers to clarify exclusions and claim triggers, as well as notification and proof of loss requirements**—Work closely with a licensed insurance broker to fully understand the coverage. Clarify what types of incidents are excluded, what conditions must be met to trigger a claim, and what the notification and documentation requirements are.

CONCLUSION

Bricking coverage is an important but often overlooked aspect of insurance, requiring careful attention to policy language and exclusions. By proactively assessing coverage needs and working closely with insurance professionals, businesses can better protect critical assets and avoid costly gaps in protection.

Contact us today for more risk management and insurance information.