INSURANCE INSIGHTS | CYBER EXCLUSIONS

Key policy exclusions leave you at risk of costly gaps in coverage.

Cyber insurance is one of the fastest growing lines of insurance. This also means the number of cyber plans and available products has also grown exponentially, but not all cyber insurance products are created equal. Coverage differences and exclusionary language amongst cyber policies has led to claims being denied, which often results in court rooms determining outcomes or large, unexpected losses that drive companies out of business.

When purchasing cyber insurance, it is important that businesses work with **experienced insurance brokers** who can help guide them through this process, as well as conduct a thorough review of the policy language. Clarifying questions around coverage, limitations and interpretations of ambiguous coverage clauses could be the difference between a covered cyber incident or not.

While not a comprehensive list of all the exclusions, we cover **six of the most common** ones— and the most prevalent causes of loss.

Exclusion:
FAILURE TO MAINTAIN MINIMUM SECURITY STANDARDS

- ☐ Clearly understand of how the insurer defines "minmum security standards" prior to taking out insurance. Depending the wording, this exclusion could give insurers cause to deny claims from almost every type of data breach.
- ☐ Coverage may be tied to security procedures identified in the insurance application. Complete applications accurately and confirm security protocols are in place for the duration of the policy period.
- ☐ Some policies contain hybrid exclusions that combine various portions of the above.

SAMPLE : WARFARE EXCLUSION

> The insurer will not be liable to make any payment in connection with an claim arising out of, or in any way attributable to, acts of war, foreign enemies, any military organization, or any government regardless of any other contributing cause or event.

Exclusion:
WAR, TERRORISM, INVASION, OR INSURRECTION

- ☐ This is a fairly standard exclusion incorporated into many classes of insurance.
- ☐ Cyber attacks from state sponsored, political or ideological origins can be construed by insurers under this exclusion language.
- ☐ Review coverage prior to taking out insurance and request to modify these exclusions to ensure coverage for "cyberterrorism" or "electronic terrorism."

Risk Cooperative

Risk. Readiness. Resilience.

1825 K St. NW, Suite 500
Washington, DC 20006
info@riskcooperative.com
www.riskcooperative.com
Phone: +1.202.688.3560
Fax: +1.202.905.0308

INSURANCE INSIGHTS | CYBER EXCLUSIONS

Key policy exclusions leave you at risk of costly gaps in coverage.

Exclusion:
WRONGFUL ACTS THAT OCCUR PRIOR TO COVERAGE

- ☐ Most policies set a "Retroactive Date" when insurer first issued a policy to the insured, so this exclusion mostly impacts new cyber policies.
- ☐ Cyber breaches are often discovered long after the breach occurred, and claims arising from a breach occurring prior to the policy's Retroactive Date may not be covered.
- ☐ Cyber policies are "claims made and reported" policies, meaning that they will only respond during the policy period. Notice of a claim must be made for coverage to exist.
- ☐ Before changing your cyber carrier, be sure to purchase an extended discovery period, to provides an additional period to report claims that would have been covered by the non-renewed policy. Alternatively, consider obtaining a Retroactive Date that predates the inception of your new policy.

SAMPLE : PRIOR ACTS EXCLUSION

The insurer will not be liable to make any payment in connection with an incident arising out of any litigation against any insured initiated prior to the respective date set forth in Item 9 of the Declarations, or involving any of the same facts, circumstances, or situations underlying such prior litigation.

Exclusion:
LOST PORTABLE ELECTRONIC DEVICES THAT RESULT IN A BREACH

- ☐ Some insurers are willing to remove this exclusion or modify it to apply only to claims arising from the loss of an unencrypted portable device.

SAMPLE : THIRD PARTY EXCLUSION

The insurer will not be liable to make any payment in connection with an incident arising out of or in any way involving, a breach of any computer system or any communication network, other than the company's computer system.

Exclusion:
THIRD PARTY PROVIDERS

- ☐ Many breaches are often the result of vulnerabilities within third party suppliers and vendors creating a big risk exposure.
- ☐ Discuss this exclusions with insurers to cofirm coverage and to what extent it will be applicable. Some policies provide limited coverage in this scenario.
- ☐ Fully understanding the exposure, and your recourse in the event of an incident, is vital to ensure you are protected.

Exclusion:
BODILY INJURY & PROPERTY DAMAGE RESULTING FROM A CYBER INCIDENT

- ☐ Beyond cyber policies, general liability and property policies exclude cyber related losses. This can make it difficult to cover losses to computers and hardware.
- ☐ Carefully review the cyber policy definition of bodily injury to verify coverage for mental anguish, mental injury, shock, emotional distress, and humiliation. Plaintiffs almost always cite these injuries as damages stemming from a data breach.

SAMPLE : BODILY INJURY & PROPERTY EXCLUSION

The insurer will not be liable to make any payment for actual or alleged bodily injury, sickness, disease, death, damage to any tangible or intangible property, including false arrest, malicious prosecution, battery, mental anguish, emotional distress, invasion of privacy, defamation, libel or slander.