Coverage Insights: Ransomware Insurance

Benefits of Cyber Liability Insurance

With ransomware attacks on the rise, the role of insurance is becoming more robust. And, although ransomware coverage has been traditionally sublimited within cyber policies, stand-alone cyber policies that cover ransomware are becoming more necessary.

In an attempt to find additional coverage for ransomware, many businesses and carriers have been turning to kidnap and ransom (K&R) policies. K&R policies have traditionally been used by organizations to protect their executives, not to protect against ransomware. Because K&R policies were not designed for ransomware, they may only provide a quick fix. K&R policies tend to be less suitable for ransomware than cyber policies and payouts tend to be lower.

Policy Definitions, Terms and Conditions

Since cyber insurance isn't standardized, organizations should review all policy language with a broker before choosing a plan that effectively covers ransomware. Policies can vary significantly in their language and coverage options, so insurance experts recommend policies that—at the very least—provide coverage for extortion demands and payments as well as lost income resulting from an attack.

Organizations should also take a close look at the following definitions, terms and conditions when choosing a policy:

- **Sublimits and deductibles** - Most policies set a sublimit for covering ransomware. It is important to review this limit carefully, considering that demands may start on the low side, but can increase quickly. Also, since making a ransom payment may make organizations a target for subsequent ransom demands within the policy year, the deductible amount should reflect that risk.
- **Payment terms** - Most policies require prior written consent before the insured can pay any ransom. This can result in payment delays and increased demands by the hackers. If an organization pays a ransom in order to resume business, without prior written consent by the insurer, there's a chance that it may not be reimbursed. Therefore, organizations need to be comfortable with a policy's terms in order to avoid compromising coverage.

- **Definition of extortion** - It is important for organizations to fully understand and agree with their insurance company's definition of extortion, since the definition dictates the trigger for coverage. For example, although hackers may intend to sell or misuse information, the ransom demand may only involve a countdown timer and demand for money. While the combination of the two may seem like an obvious threat to the insured, a carrier could possibly deny coverage on the basis that there was no explicit threat to sell or misuse information—all because of its unique definition of extortion.

What to Look for in a Policy

Companies should look for ransomware coverage that uses broad terminology and protects against a wide range of threats, including threats to do the following:

- Access, sell, disclose or misuse data stored on your network, including digital assets.
- Alter, damage, or destroy software or programs.
- Introduce malicious software, including viruses and self-propagating code.
- Impair or restrict access. Look for policies with broad terms like, "threats to disrupt business operations."
- Impersonate the insured in order to gather protected information from its clients, also known as pharming or phishing.
- Use your network to transmit malware.
- Deface or interfere with your company's website.

The Importance of Risk Management

Ransomware insurance is most effective when coupled with an effective risk management program, as there are many components in the fight against cyber crime. Risk managers should work with an insurance broker to review all applicable options before choosing cyber coverage.

For more information:

Brian Dunphy
Senior Vice President
Brian.Dunphy@alliant.com
C: 212-504-1888

Robert Horn
Co-Cyber Product Leader
Robert.Horn@alliant.com
212-504-5828

John Loftus
Co-Cyber Product Leader
John.Loftus@alliant.com
917-572-8269

