Skidmore in NLJ: Kidnap and Ransom Insurance: Unlocking Coverage for Ransomware Attacks

By Micah E. Skidmore | May 3, 2018

RELATED PRACTICES Privacy and Cybersecurity, Insurance Recovery, Litigation

The threats facing U.S. companies from cyberattacks are constantly changing, and recent media reports suggest that the era of large-scale data breaches may be giving way to more localized attacks, which promise a faster payday for cybercriminals.

In 2017, “ransomware” became a household word with the “Wannacry” outbreak, which disabled more than 200,000 computers in approximately 150 countries. Since then, there have been other isolated and large-scale ransomware events — each locking businesses and individuals out of computers and other devices unless a timely “ransom” is paid. Many cyber experts predict more to come. According to Cybersecurity Ventures, “the cost of global ransomware attacks will exceed $11.5 billion annually by 2019, up from $5 billion last year and $325 million in 2015” — a 3500 percent increase in just four years.

With this evolving threat, companies and individuals alike may ask what can be done to protect against the risk of data loss and the ransom that a cybercriminal may demand. Corporate risk managers, counsel and other executives may be tempted to assume that only a specialized network security/privacy liability policy, often colloquially referred to as a “cyber coverage,” is likely to cover such loss. There is an often overlooked alternative. Kidnap, ransom and extortion (K&R) coverage, which is often included in traditional directors and officers liability (D&O) or crime policies, may provide a much-needed source of recovery for policyholders and an efficient alternative to a dedicated cyberpolicy.

To read the full article, click on the PDF linked below.

Skidmore-Ransomware-Insurance.PDF

First appeared in *National Law Journal* April 30, 2018. (Subscription required)