haynesboone

May 3, 2018

Kidnap and Ransom Insurance: Unlocking Coverage for Ransomware Attacks

By: Micah E. Skidmore

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.

K&R Coverage for Cyber Extortion

Some K&R forms provide reimbursement for ransoms paid by corporations, but only in connection with the “kidnap,” “detention” or “hijack” of an “insured person.” Needless to say, these forms will not afford coverage for a ransomware attack on corporate computer systems. However, other K&R coverage forms are not so limited. Alternative forms may include coverage for ransom paid because of “cyber extortion.” Cyber extortion, in turn, may extend to threats to, among other things, 1. introduce malware into a computer system; or 2. alter, damage or destroy a computer program, software or data stored on such computer system, where the ransom is demanded as a condition of not carrying out the threat.

Ransomware itself may constitute evidence of malware already introduced into a computer system. Although ransomware does not typically cause “damage” to the insureds’ computer system or the data stored thereon, ransomware can alter and/or destroy programs, software and data by forever denying access to such items in the absence of the ransom requested by the cybercriminal. Appropriately worded K&R coverage forms may offer reimbursement for funds paid to restore access to computer systems and data disrupted by a ransomware attack.

Cyber Coverage for Ransomware Attacks

When it comes to insurance coverage, the potential “cyber” solutions now available in the market can seem vast and daunting. Within the past few years, most major insurance carriers have unveiled new or revised policy

forms specifically designed to protect against the burgeoning threat of cyberattacks and related liability and other risks. Although policy terms continue to vary widely, a standalone “cyber” policy may also provide coverage for ransoms paid, with the insurer’s consent, in response to an extortion threat, subject to conditions similar to those found in some K&R coverage forms.

However, depending on individual policy terms, cyber policies may have deductibles, which prohibit any substantial recovery in the event of a ransomware attack. Corporate insureds, who are specifically seeking some form of ransomware coverage in a dedicated cyber policy, should make sure that deductibles are appropriate to this objective. K&R coverage, on the other hand, may have limits and deductibles more conducive to recovery. Because not every ransomware attack involves an authorized disclosure of personal information, corporate policyholders considering a dedicated cyber policy solution should also ensure that such a disclosure is not a condition of coverage for a ransomware attack.

The Continuing Ransomware Threat

Ransomware has been a cyberthreat for more than a decade. But its surge within the last few years is the expression of a trend that is expected to carry over into 2018 and beyond.

Relative to stealing and selling individual credit card or health information, ransomware provides a more direct path to payment for cybercriminals. Even state actors have joined in extortion campaigns, and technological developments have enabled common criminals to effectively “hire” sophisticated ransomware infrastructure to stage attacks. With more and more companies (and individuals) outsourcing data storage, cybercriminals have also significant opportunities and incentives to launch ransomware attacks on the cloud.

As criminals become more sophisticated and discriminating in their targets, those businesses most dependent on timely access to data—health care providers, law firms, and government agencies—share the greatest exposure to ransomware risks in 2018.

In managing the potential risk of a ransomware attack, risk managers, in-house counsel and others expected to participate in responding to a breach event may want to consider K&R coverage and carefully review the terms of available K&R forms as an alternative to a dedicated network security/privacy liability policy.