Kidnap Ransom Insurance: Unlocking Coverage for Ransomware Attacks

March 23, 2018 Micah Skidmore

PRACTICES Privacy and Cybersecurity, Insurance Recovery, Litigation

By one account, "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 35X increase in just four years.[1] Relative to other cyber crime, ransomware is an equal opportunity enterprise—striking individuals as well as businesses of all kinds.

Risk managers, in-house counsel and other executives may be tempted to assume that there is no traditional coverage for cyber ransom, or that only a stand-alone network security/privacy liability policy (often with deductibles or self-insured retentions exceeding the ransom) is likely to cover such loss. There is an often overlooked alternative. Kidnap, ransom & extortion ("K&R") coverage, placed by many companies in connection with traditional D&O or crime policies, may provide a much-needed source of recovery for policyholders and an efficient alternative to dedicated network security/privacy liability insurance.

Ransomware Trends in 2018

Ransomware has been a cyber threat for more than a decade.[2] 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 cyber criminals. Even state actors have joined in extortion campaigns,[3] and "RaaS" ("Ransomware as a Service") platforms have enabled technically inexperienced criminals to effectively "hire" sophisticated ransomware infrastructure to stage attacks.[4] With more and more companies (and individuals) outsourcing data storage, cyber criminals have significant opportunities and incentives to launch ransomware attacks on the cloud.[5] As criminals become more sophisticated and discriminating in their targets, those businesses most dependent on timely access to data—healthcare providers, law firms, and government agencies—share the greatest exposure to ransomware risks in 2018.[6]

Coverage For Cyber Extortion

Some K&R coverage forms provide reimbursement for ransom 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. Such alternative forms may include coverage for ransom paid because of "cyber extortion." Cyber extortion, in turn, may embrace threats against an insured expressing an intention, among other things, to (1) introduce malware into the insured's 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.[7] While ransomware may constitute evidence of malware already introduced into the insured's computer system, and 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 irrevocably denying the insured access to such items in the absence of the ransom requested from the insured. 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.

A stand-alone "cyber" policy may also provide indemnification 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, K&R coverage may have limits and deductibles or self-insured retentions more conducive to recovery than what may be found in a dedicated network security/privacy liability policy. 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. If you have any questions about insurance coverage for ransomware or about K&R or cyber coverage in general, please contact one of Haynes Boone's Insurance Coverage Practice Group partners listed below.

---

[1] Jean Baptiste Su, *Acronis Releases Free Ransomware Protection for Microsoft Windows*, FORBES (Feb. 1, 2018).

[2] Trend Micro, *3 Reasons the ransomware threat will continue in 2018* (Jan. 24, 2018), ("[R]ansomware attacks have outnumbered general data breaches for the past 11 years running.").

[3] BBC News, *UK and US Blame Russia for 'malicious' Not Petya cyber-attack* (Feb. 15, 2018).

[4] Tripwire, *The Future of Ransomware 2018 and Beyond* (Dec. 26, 2017).

[5] Martin Giles, *Six Cyber Threats to Really Worry About in 2018*, MIT TECHNOLOGY REVIEW (Jan. 2, 2018).

[6] Anna Liska, *5 Ransomware Trends to Watch in 2018*, RECORDED FUTURE BLOG (Mar. 6, 2018).

[7] Travelers Form KER-16001 (07-16 ed.).