TRAUB LIEBERMAN

CYBER LAW BLOG

February 10, 2020

Maryland District Court Finds Coverage for Ransomware Attack Under Businessowners' Policy

BY: Jason Taylor

The term "silent cyber" is a popular catch-phrase at the moment. The term generally refers to potential cyber-related losses covered under traditional property and liability policies that were not specifically designed to cover cyber risk. Older forms were not intended to provide such coverage, and most likely, cyber-related risks were not considered (or considered seriously) at the time such policies were issued. Understandably, carriers are hesitant to advance coverage for risks and losses never contemplated or intended under traditional policies. Creative policyholders and their attorneys, however, will look everywhere for coverage in the event the policyholder failed or was unable to secure cyber-related coverage for a specific loss. A recent decision from the U.S. District Court in Maryland arguably fits into this "silent cyber" category.

In *Nat'l Ink & Stitch, LLC v. State Auto Prop. & Cas. Ins. Co.,* 2020 WL 374460 (D. Md. Jan. 23, 2020), the insured brought a coverage action against its businessowners' insurance carrier, State Auto, seeking coverage for damage sustained to its computer system in a ransomware attack. The ransomware attack allegedly prevented the insured from accessing all of the art files and other data contained on its server and most of its software. The attacker demanded payment of a bitcoin to release access to the software and data. Although the insured made the requested payment, the attacker demanded further payment and refused to release the software and data. The insured employed a security company to replace and reinstall its software, and to install protective software on its computer system. In the end, although the insured's computers still functioned, the installation of protective software slowed the system and resulted in a loss of efficiency. The art files formerly stored on the server could not be accessed, and had to be recreated. The computer experts also testified that there were likely dormant remnants of the ransomware virus in the system that could "re-infect the entire system."

State Auto denied coverage for the cost of replacing the insured's computer system. The policy provided coverage "for direct physical loss of or damage to Covered Property." The policy included a "Businessowners Special Form Computer Coverage" endorsement that defined "Covered Property" to include "Electronic Media and Records (Including Software)," and defined "Electronic Media and Records" to include: (a) electronic data processing, recording or storage media such as films, tapes, discs, drums or cells; and (b) data stored on such media.

The parties disputed whether the insured experienced "direct physical loss of or damage to" its computer system, to justify reimbursement of the replacement cost for the entire system under the Policy. State Auto argued that because the insured only lost data, an intangible asset, and could still use its computer system to operate its business, it did not experience "direct physical loss" as covered by the Policy. The District Court disagreed, finding that the Policy's language contemplated computer data and software to be property subject to "direct physical loss," and that its computer system itself sustained damage in the form of impaired functioning. Consequently, the insured could recover based on either (1) the loss of data and software in its computer system, or (2) the loss of functionality to the computer system itself.

The District Court first had to answer whether data or software can be susceptible to physical loss or damage. The costs sought by the insured were the replacement costs for its hardware and software — in other words, its entire computer system. Thus, the insured did not seek solely the costs of replacing its customer data, but rather, sought a fully functioning computer system not (1) slowed by the necessary remedial and protective measures, or (2) at risk of reinfection from a dormant virus. Importantly, the Policy did not limit coverage to "tangible property." According to the District Court, the Policy expressly listed "data" as an example of Covered Property under its definition of "Electronic Media and Records (Including Software)." The Policy also contained the phrase "Including Software" in its heading describing covered property. Thus, the court reasoned that the plain language of the Policy contemplated that "data" and "software" are covered and can experience "direct physical loss or damage."

State Auto also argued that because the server still functioned to conduct new business, albeit more slowly, the insured did not suffer a direct physical loss or damage. The District Court found, however, that State Auto's argument neglected the plain language of the Policy, which protected against not only "physical loss" but also "damage to" both the media and the data. The court reasoned that while the computer system retained residual ability to function, it had been rendered slow and inefficient, and its storage capability was damaged such that its contents (i.e., the data and software) cannot be retrieved. In examining case law from other jurisdictions, the District Court found persuasive cases suggesting that loss of use, loss of reliability, or impaired functionality demonstrated the required damage to a computer system consistent with the "physical loss *or damage to* " language in the Policy. According to the District Court, in many instances a computer will suffer "damage" without becoming completely inoperable. In this case, not only did the insured sustain a loss of its data and software, but was left with a slower system, apparently sheltering a dormant virus, and was unable to access a significant portion of software and stored data. State Auto was unable to point to any case law that held for damage to be covered a computer system must be completely and permanently inoperable. The District Court found that the plain language of the Policy provided coverage for such losses and damage, and granted summary judgment in favor of the insured's interpretation of the Policy terms.

While *National Ink* arguably falls within that category of "silent cyber" -- in that the standard businessowners' policy form at issue was not specifically intended to provide coverage for ransomware or other cyber-attacks -- the policy language at issue is important. The policy language considered by the District Court included some important features that the court deemed compelling. The Policy defined "Covered Property" to include "Electronic Media and Records *(Including Software)*," and defined "Electronic Media and Records" to include not only electronic data processing, recording or storage media, but also the "[d]ata stored on such media." As computer-related attacks have become more prevalent, policy language has evolved. Newer businessowners'' forms, for example, specifically exclude cyber-related losses, or include specialized coverage endorsements or sub-limits. *National Ink*, however, is a reminder that until older or unclear policy language is adapted to meet current threats, coverage for cyber- or other computer-related attacks may still be lurking in more traditional policy forms.