After a Ransomware Attack, Does Property Insurance Cover Damaged Software and Hardware?

Prepared by:
Scott Godes
Barnes & Thornburg LLP

LORMAN®

Published on www.lorman.com - July 2020

INTRODUCING

Lorman's New Approach to Continuing Education

ALL-ACCESS PASS

The All-Access Pass grants you UNLIMITED access to Lorman's ever-growing library of training resources:

- ☑ **Unlimited Live Webinars** - 110+ live webinars added every month
- ☑ **Unlimited OnDemands** - Over 3,900 courses available
- ☑ **Videos** - More than 1,900 available
- ☑ **Slide Decks** - More than 3,300 available
- ☑ **White Papers** - More than 2,000 available
- ☑ **Reports**
- ☑ **Articles**
- ☑ **... and much more!**

Join the thousands of other pass-holders that have already trusted us for their professional development by choosing the All-Access Pass.

Get Your All-Access Pass Today!

SAVE 20%

Learn more: **www.lorman.com/pass/?s=special20**

Use Discount Code Q7014393 and Priority Code 18536 to receive the 20% AAP discount.

*Discount cannot be combined with any other discounts.

After a Ransomware Attack, Does Property Insurance Cover Damaged Software and Hardware?

February 11, 2020 | Policyholder Protection, Cyber Insurance, Policy, Data Security

Scott N. Godes

Partner / Data Security and Privacy Co-Chair

Barnes & Thornburg LLP

Do traditional insurance policies provide coverage for losses due to cyberattacks and cybersecurity events? That question is the so-called "silent cyber" issue in a nutshell. "Silent cyber" is the idea that coverage for cybersecurity-based losses can be found outside of cyber insurance policies.

A recent decision from a federal court in Maryland says that, yes, it can. The court ruled that an insurance company must cover the costs of software, data, computers, and servers that were lost or damaged by ransomware under the property insurance coverage of a businessowner's insurance policy.

What happened?

In *National Ink & Stitch, LLC v. State Auto Property & Casualty Co.*, No. 18-2138, slip op. (D. Md. Jan. 23, 2020), a policyholder and its insurance carrier disputed whether a businessowner's insurance policy (often referred to as a BOP) provided "coverage for damage alleged to have been sustained to [the policyholder's] computer system in a ransomware attack." The policyholder, National Ink & Stitch, LLC, is an embroidery and screen-printing business. National Ink stored art, logos, and designs, as well as various types of software, on its computers and servers.

National Ink fell victim to a ransomware attack. Because virtually all of its files and software were locked up, and its computers unusable for their intended purpose, National Ink decided to pay the ransom. Unfortunately, it had to pay twice before it ultimately was able to get its software and at least some data unlocked.

After it got the "keys" to unlock its files, National Ink's computers still functioned, but the company installed protective software that slowed the system and resulted in a loss of efficiency. National Ink was not able to recover its art files, and there was a risk that there were remnants of ransomware on its computers. So, National Ink was left with the choice of either wiping everything off of its servers or buying a new server and related hardware.

The insurance company refused to cover the cost of replacing the computer system

National Ink sought coverage under its businessowner's insurance policy. That insurance policy covered "direct physical loss of or damage to Covered Property." It also had a "Businessowners Special Form Computer Coverage endorsement." That endorsement provided coverage for "Electronic Media and Records (Including Software)," and that included "(a) Electronic data processing, recording or storage media such as films, tapes, discs, drums or cells; [and] (b) Data stored on such media."

The costs for which National Ink sought coverage were "the replacement costs of its hardware and software – in other words, its entire computer system." National Ink wanted "a fully functioning computer system not (1) slowed by necessary remedial and protective measures, or (2) at risk of reinfection from a dormant virus."

Rather than agree to provide coverage, State Auto pulled an argument straight out of the proverbial playbook of many insurance carriers and asserted that it need not cover the cost of replacing National Ink's computer system. It argued that because National Ink "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 court ruled that State Auto has to cover losses due to ransomware under the property insurance coverage parts of the businessowner's policy.

The court's early summary of its holding is important. It stated, "As detailed below, Plaintiff can 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."

Ransomware caused physical damage to software

The court went on to explain that "the plain language of the [businessowner's] Policy contemplates that data and software are covered and can experience 'direct physical loss or damage.'" The court then explained that "Maryland courts would find physical damage to [National Ink's] computer software, despite its installation on [National Ink's] computer system, because the software was rendered entirely unusable by the ransomware attack." Those two statements from the court illustrate an important point: *ransomware can cause direct physical loss to data and software.*

Ransomware damaged computer hardware

The court went on to require State Auto to cover the costs of lost hardware. Specifically, the court ruled that National Ink "has also demonstrated damage to the computer system itself, despite its residual ability to function." The court further determined "that loss of use, loss of reliability, or impaired functionality demonstrate the required damage to a computer system, consistent with the 'physical loss or damage to' language in the Policy."

The court flat rejected the frequent insurance company argument about covering damage to computers: "Indeed, in many instances, a computer will suffer 'damage' without becoming completely inoperable. Here, not only did Plaintiff sustain a loss of its data and software, but Plaintiff is left with a slower system, which appears to be harboring a dormant virus, and is unable to access a significant portion of software and stored data." It is difficult to overstate the importance of that point: *ransomware damaged the computer hardware, even though the computers still had the residual ability to function.*

As part of its analysis, the court evaluated the cases that the insurance company cited and decided that the decisions were not persuasive. One point that does not appear to have been made in the decision is that many states recognize that a split in authority on an issue is evidence of ambiguity in the insurance policy language. Insurance law, in many states, holds that ambiguous policy language is interpreted in favor of coverage and construed against the insurance carrier.

What does this mean for corporate policyholders and insureds?

There are several takeaways from the *National Ink & Stitch, LLC v. State Auto Property & Casualty Co.* decision.

1. **Silent cyber is real.** The insurance industry reportedly is trying to figure out how to clearly include or exclude coverage for cyber risks, or even figure out how to address the issue. While the industry struggles with changing its

policy language, this decision shows that other insurance policies can provide coverage for losses due to cyberattacks.

2. **A best practice is to think broadly about coverage for cyber risks when a claim hits.** If an entity suffers a cyberattack, is a cyber insurance policy the only potential source of coverage? This decision is a good reminder that the answer is no. A best practice is to continue to seek coverage for these losses under a cyber insurance policy, because a well written cyber insurance policy should provide coverage for losses like this. Even if a cyber insurance policy provides coverage, it might not provide full coverage for the losses. This decision reiterates that a property policy can provide coverage for losses from a cyberattack, including damage to hardware and software.

3. **It can be worth going to court to enforce a policyholder's rights to coverage.** This case illustrates an unfortunate truth: sometimes, a policyholder has to go to court to get the coverage that it believes it is due for a loss.