Third-Party Liability for Ransomware Attacks, Are You Covered?

Daily Business Review
12.2.20

This article appeared in the Daily Business Review on December 2, 2020.

Commentary provided by Oliver Sepulveda.

The COVID-19 pandemic has caused a massive shift in the way organizations do business and the way their employees do their work, but, as is often the case, this shift has brought about an increase in cybersecurity risks, which should not be overlooked. Much of this increased risk comes from the rise of ransomware attacks. According to one of the largest cyber insurance providers in North America, approximately 41% of cyber insurance claims in the first half of 2020 are attributed to ransomware attacks. While one can be forgiven for thinking that cybersecurity is only a concern for large corporations, that is far from the case. The malicious actors behind ransomware attacks do not discriminate. It is a problem that affects organizations large and small in various industries including health care, government, construction, manufacturing, legal, and education, to name a few. Despite this increased risk, cybersecurity companies report that more than a quarter of small businesses have no plan to mitigate a ransomware attack.

For the uninitiated, ransomware is a type of malicious software that is embedded into a computer system through a variety of different methods. It encrypts the data on that system, potentially rendering that system, and any other systems that rely on that data, inoperable. The ultimate goal of the malicious actors is to extort money, a ransom, from the victim by offering to restore the computer systems upon payment. Victims can either pay the ransom or deal with the fallout; many, at the suggestion of their cyber insurance carriers, opt to pay the ransom.

Unfortunately, when faced with a possible ransomware attack, organizations need to consider the unintended victims and the potential for liability to reliant third parties if their computer systems remain inoperable or their data is lost. Recently, a hospital in Germany was a victim to a ransomware attack which caused the need for an emergency transport of a number of patients due to the inoperable computer systems. Tragically, one of the patients died during transport and is reported to be the first known death caused by a ransomware attack. And Blackbaud, a leading cloud services provider, is facing numerous class action lawsuits as a result of a ransomware attack on its servers. As small businesses rely more and more on computers and data rather than paper, these unintended consequences are likely to become more frequent, and, while organizations often look to their general liability policies to cover them for accidental losses, they may find themselves up a creek without a paddle.

Third-Party Liability for Ransomware Attacks, Are You Covered?

Many, if not most, commercial general liability policies expressly preclude coverage for data related liabilities. However, even if your policy does not exclude data related liability, you may still have a hard time obtaining coverage for such an event.

General liability policies typically offer to defend the insured faced with a lawsuit claiming either bodily injury or property damage caused by an occurrence (typically defined as an accident). Bodily injury is fairly easy to identify and clever plaintiffs can usually get around the need for an occurrence by pleading some form of negligence (i.e., negligent failure to provide security). However, a ransomware attack is far more likely to cause property damage (i.e. corrupted data and unusable computer systems) than bodily injury, and most courts around the country do not interpret corruption of software and data as property damage under traditional insurance policies.

Recently though, a federal district court in Maryland held that loss of computer data and software was covered. There, the insured, an embroidery and screen-printing business, was the victim of a ransomware attack and, despite paying the initial ransom, was unable to recover many of the files that it used to run its business. The company looked to its insurance to cover its own losses and the insurer denied coverage because, according to the insurer, it had not suffered a physical loss or damage to its computer system. The court disagreed and noted that unlike many other insurance policies, the policy at issue did not limit coverage to damage to "tangible property" and, in any event, it reasoned that Maryland courts would find physical damage to the computer software because the ransomware attack rendered the software inoperable.

This is one of first instances of coverage for lost data resulting from a ransomware attack under a traditional policy, but it may not be the last. That said, this is a minority position and the policy language was a determining factor in this case.

Given the heightened risk for ransomware attacks during the pandemic, organizations should not rely on the remote possibility that a court may rule in its favor on these issues. The most prudent thing to do is to prevent these issues from arising in the first place. Indeed, when it comes to cyber attacks, an ounce of prevention is worth a pound of cure, but no cybersecurity plan is foolproof; technology changes at such a rapid pace that the risk of an attack is always present. Rather than depend on general liability coverage, which may not cover cyber risks, organizations should consider adding cyber insurance to their insurance portfolio. These coverages, however, are far from standardized and come in a variety of shapes and sizes. For example, some cyber policies may provide coverage for expenses incurred in responding to a ransomware attack but may not provide coverage for any damage caused to third parties. Other policies may cover liability but may not provide coverage when the attack is through an employee-owned device.

Now that work-from-home has become ubiquitous, companies, big and small, should carefully evaluate their insurance portfolios and fill any gaps that they may have due to the heightened risk that this new work arrangement brings.

Third-Party Liability for Ransomware Attacks, Are You Covered?

Oliver Sepulveda *is an associate in the Miami office of Shutts & Bowen, where he is a member of the insurance practice group.*

Professionals

Oliver Sepulveda

Practice Areas

Cybersecurity and Data Privacy Task Force

Insurance

Industries

Insurance

Offices

Miami