Published on *The National Law Review* https://www.natlawreview.com

The MOVEit Hack, Ransomware Attacks, and Cyber Insurance

Article By:

Jeffrey J. Meagher

Hudson M. Stoner

US Litigation and Dispute Resolution Alert

Ransomware attacks and cyber data theft are an unfortunate fact of life for businesses. Whether through attacks targeting individual companies or widespread campaigns carried out by exploiting vulnerabilities in third-party software, such as the 2021 SolarWinds attack and the recent MOVEit hack, cyber criminals are engaging in more frequent and more sophisticated cyber extortion schemes. Regardless of whether victims pay ransom, and many do not, the attacks can be costly and highly disruptive for a business. The question for most companies is not whether an attack will happen, but when and how the business can best respond. This article discusses several insurance-related issues that policyholders should consider as they plan for the potential impact of an attack on their organizations.

THE MOVEIT HACK

Earlier this summer, the Russian-linked CL0P ransomware gang exploited a “zero-day” or previously unknown vulnerability in MOVEit Transfer, a popular file-transfer service used by organizations around the world to move large amounts of often-sensitive data.[1] This vulnerability allowed the attackers to access and steal customers’ data, which the group then began using as leverage for ransom demands. According to Coveware, a leading cyber extortion response firm, most victims of the attack chose not to pay a ransom, but those that did pay a ransom paid a significant amount.[2] In addition, the ransomware group behind the attack has started publishing some of the information stolen in the attack in an effort to encourage payment.

NOTICE

One of the first issues policyholders should consider in connection with any cyberattack is notice. Most cyber insurance policies require the policyholder to provide the insurer with notice of a cybersecurity breach as a condition to coverage. Many policies require notice to be given “as soon as practicable” after discovery of the breach, while some policies require notice to be given during the policy period or within a certain number of days after the policy period ends. Notice provisions are

important for policyholders to understand because an insurer may deny an otherwise valid claim based on late notice. Many states require an insurer to prove that it was prejudiced by the late notice to prevail on a late-notice defense, but some states do not. Accordingly, policyholders should be aware of the notice provisions in their cyber insurance policies (and any other policies that may provide cyber coverage) and provide notice of cybersecurity breaches in accordance with those provisions.

BREACH RESPONSE COSTS

Cyber insurance policies typically provide a mix of first-party and third-party insurance coverage. First-party insurance provides coverage for losses suffered by the insured, while third-party insurance provides coverage for the insured's liability for losses suffered by third parties. One of the most important grants of first-party coverage for policyholders in the early stages of responding to a cyberattack is the coverage grant for breach response costs. Although different cyber policies use different terms, most cyber policies provide coverage for certain costs incurred as a result of a cybersecurity breach. For example, most cyber insurance policies provide coverage for reasonable and necessary expenses incurred by a policyholder to investigate the cause and extent of a breach. Most cyber policies also provide coverage for expenses incurred to notify customers or employees whose personal information may have been stolen by the attackers. In addition, many cyber policies provide coverage for legal expenses incurred to comply with breach notice laws. As policyholders assess the fallout from the MOVEit hack, they should be aware of what type of breach response costs their insurance policies cover and keep their insurers apprised of the remedial actions being taken to the extent required or appropriate.

RANSOMWARE SUBLIMITS

Most cyber insurance policies also provide coverage for cyber extortion payments (i.e., ransoms). As ransomware attacks have become more common, however, many insurers have introduced ransomware sublimits in an attempt to limit their exposure to such attacks. A sublimit is a lower limit that applies to a particular type of loss. Thus, for example, a cyber policy may have a US$10 million limit that applies to most losses and a US$1 million sublimit that applies to ransomware losses. Insurers sometimes argue that all of the costs associated with a ransomware attack are subject to a ransomware sublimit even though the policy provides only that costs arising out of a ransom event (often defined as a threat or series of threats to commit or continue an attack unless the policyholder pays a ransom) are subject to the sublimit. Policyholders should carefully review their cyber insurance policies before making a claim to determine whether certain costs (particularly costs incurred in connection with the security breach that typically precedes a ransom demand) fall under insuring agreements that are not subject to a ransomware sublimit.

CONCLUSION

The MOVEit attack is an important reminder that even the most sophisticated companies remain vulnerable to cyberattacks with potentially serious economic consequences. Cyber insurance is one way to address that risk, but it is only effective if it provides coverage when called upon. Accordingly, policyholders should review their cyber insurance programs, consider the issues discussed above, and decide whether they are adequately protected.

FOOTNOTES

[1] Fed. Bureau of Investigation & Cybersecurity & Infrastructure Sec. Agency, Joint Cybersecurity Advisory, #StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability (June 16, 2023), https://www.cisa.gov/sites/default/files/2023-07/aa23-158a-stopransomware-cl0p-ransomware-gang-exploits-moveit-vulnerability_8.pdf.

[2] *Ransomware Monetization Rates Fall to Record Low Despite Jump In Average Ransom Payments*, COVEWARE (July 21, 2023), https://www.coveware.com/blog/2023/7/21/ransom-monetization-rates-fall-to-record-low-despite-jump-in-average-ransom-payments.

National Law Review, Volumess XIII, Number 254

Source URL:https://www.natlawreview.com/article/moveit-hack-ransomware-attacks-and-cyber-insurance