Kaseya Data Breach Is Another Signal to Cyber Underwriters about the Dangers of Ransomware Attacks

PLUS Blog
Posted on July 19, 2021, by PLUShq
David Shannon, Esq.

In early July, Kaseya, a software supplier based in Miami, Florida, was the victim of a sophisticated ransomware attack. This attack was even more damaging because the hackers targeted an IT management software supply vendor. Kaseya provides software as a service (SaaS) and virtual server administrator systems (VSA) to numerous managed service providers (MSP). The MSPs use Kaseya's software systems to assist with their numerous business customers in implementing and managing their computer systems.

The Kaseya data breach was purportedly carried out by the hacking group Revil. The ransomware virus was injected into a Kaseya software update that was sent to its customers. A chain of events then occurred where the virus infected the MSPs and then numerous business clients of the MSPs. Several thousand businesses (likely to increase) have been impacted and found most or all of their computer systems encrypted.

The cyber claims for this will be significant. All of the businesses will be making claims for first-party data breach response expenses. In addition, it is likely that third-party claims against the MSPs will also be occurring in the near future.

Cyber underwriters should learn from this exploitation breach, as well as earlier supply chain breaches, like Solar Winds, that a breach of one insured, particularly an MSP, can lead to significantly more companies being impacted and significantly more claims, risks and expenses. Underwriters working with MSPs need to fully evaluate a company's computer systems, the vendors and suppliers they use, the number of customers they have and the number of endpoints these customers have. A forensic exam always begins with determining the total number of endpoints, i.e. servers, workstations or other computer systems, that will need to be reviewed, potentially cleaned and undergo remediation services.

While the cyber policy may be written simply for the MSP insured, the claims that could arise in the future will be for the dozens, if not hundreds, of customers the MSP insured works with. Cyber underwriters would be well advised to develop policies that will examine the key areas of an MSP's supply chain. The business security practices, supply chain, system controls, backup and siloing, or containment, of different systems must be reviewed to determine the full risk that exists. While both the third-party computer system providers and their end users must develop a mindset of security and containment, cyber

underwriters must also be evermore vigilant in determining whether these practices have been implemented and determine the full effect if a supply chain attack occurs.

David Shannon, Esq., chairs both the Privacy and Data Security Practice Group and the Intellectual Property, Technology and Media Litigation Practice Group at Marshall Dennehey Warner Coleman & Goggin. He concentrates a substantial portion of his practice on privacy law, data breaches, intellectual property, copyright and trademark infringement, as well as trade secret, trade dress technology and media related litigation. He may be reached at djshannon@mdwcg.com.