Portfolio Media. Inc. | 111 West 19th Street, 5th floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Kaseya Ransomware Hit Casts Wide Net Of Potential Liability

By **Ben Kochman**

Law360 (July 9, 2021, 8:42 PM EDT) -- A cyberattack on software vendor Kaseya that led to a widespread ransomware spree may also cast a wide net of liability, with regulators and potential plaintiffs likely to question whether Kaseya took reasonable steps to prevent the attack and if victims appropriately vetted their vendors.

In the wake of the attack, which the Miami-based software company says impacted up to 1,500 organizations across the globe, U.S. regulators may urge victims to disclose whether they've been affected and threaten enforcement for companies that keep their involvement secret, cybersecurity attorneys say. Class action attorneys, meanwhile, could home in on whether ransomware victims — many of which are believed to be small and mid-size businesses without massive cybersecurity budgets — reasonably scrutinized the security practices of their IT providers that had been using Kaseya's vulnerable software.

"If you properly vet a vendor, you would think that they have appropriate security measures in place to mitigate this from occurring, so the question is what type of diligence did you do and did you miss it because it wasn't enough?" said Jason Johnson, a partner in the privacy and cybersecurity practice at Moses & Singer LLP.

"For small businesses or startups, however, real due diligence costs money and time, resources that they don't always have," Johnson added.

Kaseya itself is likely to face questions about what security measures it had in place before the attack, and to what degree it heeded a Dutch security researcher group's April warning about security vulnerabilities lurking within its network. The group, the Dutch Institute for Vulnerability Disclosure, wrote in a Wednesday blog post that Kaseya had worked together with its researchers to recently release fixes resolving several of the discovered flaws, calling the company's response "on point and timely."

However, "one of the two vulnerabilities" used in the cyberattack "was one we previously disclosed" to Kaseya, the group added.

"If vulnerabilities are known to you, and you don't take what a jury or a judge or regulator could consider to be a reasonable course of action to address them, regulators or class action lawyers will seize on those kinds of mistakes," said John Reed Stark, a data breach response and digital compliance consultant and senior lecturing fellow at Duke University School of Law.

"I hate the whole notion of 'gotcha' as it regards to cybersecurity incidents, because

there's always a 'gotcha,' and that's why these class actions are so successful," Stark added. "There's no way to be perfect. No one's going to bat 1.000."

In a video statement **released to the public,** Kaseya CEO Fred Voccola has said that attackers targeted its virtual systems/server administrator, or VSA, product, which is used by companies that provide remote IT services to between 800,000 and 1 million entities around the globe. A company representative did not immediately respond Friday to a request to comment on the timeline Kaseya used to address the vulnerabilities reported by the Dutch group.

Up to 1,500 organizations are believed to have been"directly impacted" by the attack, which was discovered right before the start of the U.S. July 4 holiday weekend, Voccola said in the video, adding that the company followed its playbook and quickly shut down its VSA product within an hour of receiving reports of suspicious activity.

As of Friday, self-confirmed victims of the attack included the Swedish grocery chain Coop, the town governments of North Beach and Leonardtown, Maryland, and 11 schools in New Zealand. Cybersecurity experts have said the scope of the attack rivals that of a May 2017 ransomware attack known as "WannaCry" that hit hospitals, telecoms and other businesses **around the globe,** affecting computer systems in 150 countries. An affiliate of the Russia-linked cybercriminal gang known as REvil — which the FBI says was behind a Memorial Day weekend cyberattack on global meat supplier JBS that spurred an **$11 million ransom** payment — has claimed credit for the episode.

Depending on which sectors the ransomware victims are in, federal or state regulators are likely to ask them for information on to what extent they vetted the security of their IT providers, attorneys say. Cybersecurity experts say that doing due diligence on any third-party vendor is a best practice, given that hackers often **target vendors** as a way to potentially hit many of their clients at once.

"Of course companies are going to ask their vendors a lot of questions about cybersecurity, just like you'd expect to ask a locksmith, 'Who has the keys to this lock, and what are the vulnerabilities to it?'" said Kelvin Coleman, executive director at the National Cyber Security Alliance, a nonprofit that runs cybersecurity trainings in the public and private sectors.

Once the dust settles, ransomware victims may also receive inquiries from the U.S. Securities and Exchange Commission, which has recently taken a more active role in pursuing information on cyberattacks in the software industry, said Stark, who spent 18 years in various roles at the SEC, including 11 as the founder and chief of the agency's Office of Internet Enforcement.

The agency is currently investigating whether companies failed to disclose the effects of December's now infamous SolarWinds Corp. cyberattack on their businesses, **offering amnesty** to those that come forward and potential enforcement actions and steep fines for those that don't.

"The SEC is clearly very motivated to make sure that any company that experiences any impact from any supply chain attack better be disclosing that accurately to shareholders," Stark said.

Any sort of disclosure of a data security incident can provide ammunition for class action attorneys, some of whom "shoot first and ask questions later" after learning of the existence of a ransomware attack, said Al Saikali, chair of the data security and

privacy group at Shook Hardy & Bacon LLP.

"We'll likely see class action lawsuits against companies that were victimized by this latest ransomware spree, and that's unfortunate," Saikali told Law360. "Such lawsuits do nothing but create a disincentive to companies disclosing these incidents, which ultimately harms the data subjects."

-- Additional reporting by Al Barbarino. Editing by Emily Kokoll.
