NOT "IF" BUT "WHEN"—THE EVER INCREASING THREAT OF A DATA BREACH IN 2021

Date: 14 July 2021

Litigation and Dispute Resolution Alert

By: Victoria Forson, Tyler G. Anders, Caroline H. Boone, Desiree F. Moore

FOURTH OF JULY DATA BREACH

The latest in a recent string of high profile and wide-reaching cyber-attacks occurred over the fourth of July weekend. A criminal hacking enterprise known as REvil launched a sophisticated cyberattack involving a Florida-based software vendor named Kaseya that impacted some of Kaseya's customers.[1] Kaseya provides software solutions for managed software providers and IT departments to enable them to remotely monitor, manage, automate, and secure all of their IT services.[2] Kaseya provides regular system updates to its customers to ensure the security of its systems. In this case, however, the attackers took advantage of a vulnerability in Kaseya's VSA on-premises products and pushed malicious software that infected the customer's systems.[3] According to CNN, the attackers requested a ransom of US$70 million in exchange for the decryption key.[4] The attack reportedly compromised the data of between 800 and 1,500 companies around the world, though it will likely take several more days to understand the full extent of the attack's ramifications, given that many businesses were closed over the holiday weekend.[5]

DATA BREACH STATISTICS IN 2021

Data breaches such as the one experienced by Kaseya have increased significantly in recent years. According to the FBI's 2020 Internet Crime Report, the Internet Crime Complaint Center received 791,790 cybercrime complaints in 2020, with reported losses exceeding US$4.1 billion.[6] This record number of complaints represents a 69 percent increase in total complaints over 2019 alone. What is even more alarming is that experts say that the sophistication of the threats from these cyberattacks has also significantly increased, thanks to the application of emerging technologies such as machine learning, artificial intelligence, and 5G.[7] The 2020 “SolarWinds” attack highlighted the reality of this increasing sophistication—for more than nine months, Russian military hackers had access to digital files of the U.S. Departments of Justice, State, Energy, Commerce, and the U.S. Treasury, after sabotaging a piece of computer code buried in a software called SolarWinds.[8] The increasing “tactical cooperation” between hacker groups and state actors evidenced by the SolarWinds attack is another example of cybercrime's increasing threat.[9]

NOT “IF” BUT “WHEN”

If the statistics are correct, the question for most companies is not *if* they will be a victim of cybercrime, but *when*. When a company experiences a data breach, the immediate aftermath can be hectic—companies often find that

they are scrambling to answer key questions like what information was accessed, who gained access, whether individuals are at risk, and to act quickly to mitigate the damage.

Companies must also be prepared to comply with the legal obligations to individuals, state attorneys general, and other regulatory bodies in the aftermath of a breach—a task that is often daunting in the midst of an already stressful situation. Every state, the District of Columbia, Puerto Rico, and the Virgin Islands has enacted legislation requiring notification of security breaches that involve personal information, and, depending on the types of information involved in the breach, other laws or regulations may impose additional obligations. Global requirements to protect information proactively further complicate this issue. In many circumstances, companies are under strict timelines to notify impacted individuals and report the breach to the authorities, credit-reporting agencies, and more.

RESPONDING TO A BREACH

While preventing all manner of data breach outright is nearly impossible, companies that work closely with legal counsel to prepare data breach response plans, including how notification will flow internally and with outside counsel and other vendors in the immediate aftermath of an incident, are better positioned to respond to a breach swiftly and in a streamlined fashion. Tabletop exercises to practice what is set forth in the plan are also key to ensuring a well-managed response.

Even where clients have not put a plan in place, a data security incident or breach can be navigated smoothly and with minimal damage to the company. With the support of legal counsel, a well-orchestrated data breach response includes notifying key stakeholders in a timely fashion, liaising with insurance to maximize coverage, and engaging experienced and capable vendors to perform a forensic analysis without delay. Experienced legal counsel will also assess regulatory obligations and guide clients through the initial notification process and any follow up correspondence with data subjects, regulators, and more. In all instances, it is critical to work alongside counsel to comprehend the magnitude of the incident and navigate the incident with direction, decisiveness, and clarity.

FOOTNOTES

[1] https://www.kaseya.com/potential-attack-on-kaseya-vsa/.

[2] https://www.kaseya.com/products/vsa/.

[3] https://www.theguardian.com/technology/2021/jul/06/kaseya-ransomware-attack-explained-russia-hackers; https://us-cert.cisa.gov/kaseya-ransomware-attack.

[4] https://www.cnn.com/2021/07/06/tech/kaseya-ransomware-what-we-know/index.html.

[5] https://www.nytimes.com/live/2021/07/06/business/economy-stock-market-news#kaseya-cyberattack-ransomware-revil.

[6] https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf.

[7] https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=52febf0958d3.

[8] https://www.cbsnews.com/news/solarwinds-hack-russia-cyberattack-60-minutes-2021-07-04/.

[9] https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/?sh=52febf0958d3.

KEY CONTACTS

VICTORIA FORSON
PARTNER

DALLAS
+1.214.939.5716
VICTORIA.FORSON@KLGATES.COM

TYLER G. ANDERS
ASSOCIATE

NASHVILLE
+1.615.514.1805
TYLER.ANDERS@KLGATES.COM

