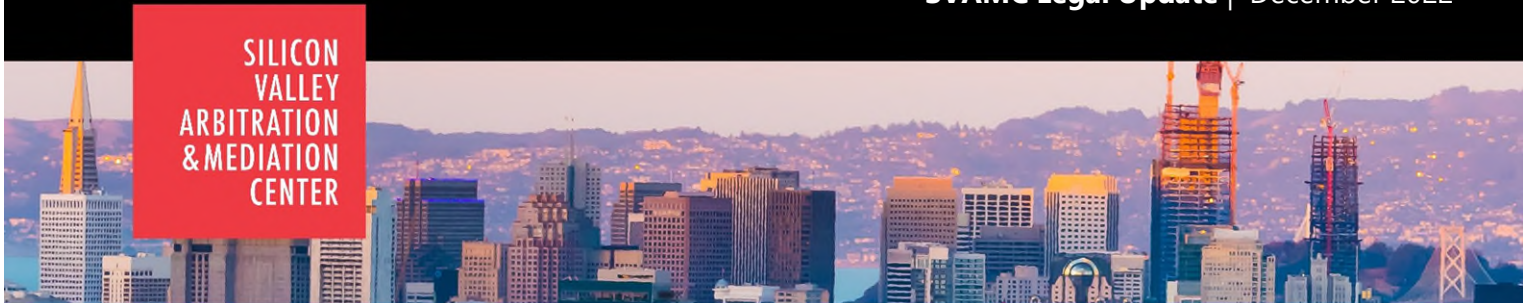

Cyberattack – Force Majeure?

Introduction

Cyberattacks happen. A hacker may enter a company's system via e-mail as a phishing scheme. Another may compromise a company's software that manages data storage. Regardless of how it's done, malware infection rates have increased over the years. As a result of various catastrophic state backed cyber-attacks, Lloyd's of London intends to exclude them from cyber-insurance policies. Regardless of the entry point, however, identifying the source of a cyberattack can be difficult. This is relevant for arbitration. Some courts have indicated a state sponsored cyberattack may qualify as a force majeure event. What is more, a party may, depending on the contractual language, avoid arbitration by terminating an agreement due to force majeure. This article will explore how to potentially avoid some of these issues.

Force majeure

In New York, at least, an event cannot be force majeure unless it's specifically provided for in the contract. However, even then, a contract may specify more generally that acts of "sabotage, terrorism, [and] vandalism" or "similar causes beyond the control of such party" constitute such an event. Regardless, courts generally require under the common law that the occurrence be something that was unforeseeable or beyond their control. So if a party to a contract didn't take reasonable precautions to prevent the alleged force majeure event, it will less likely qualify.

Not many courts have addressed the issue of whether a state sponsored cyberattack is force majeure. In *Princeton Cmty. Hosp. Ass'n v. Nuance Commc'ns, Inc.*, No. 1:19-00265, 2020 WL 1698363, at *5 (S.D.W.Va. April 7, 2020), the court assumed – without deciding – that a state sponsored malware attack could constitute force majeure. The clause excused non-performance if "that performance is rendered impossible by . . . *governmental acts* or orders or restrictions, acts of terrorism . . . war." (Emphasis added) Whether a cyber-attack can be force majeure depends in large part on the arbitration clause wording.

Escape clauses

Generally, a contractual arbitration clause requires that the parties submit to the specified forum. This is where the Federal Arbitration Act applies. Subject to certain limitations, it mandates that parties in such cases submit to the arbitration forum.

But there is a way to try and escape the Act even when the limitations don't apply.

Depending on how a force majeure clause is written, it may permit termination of the contract upon its occurrence. Some, like in *Commonwealth Edison Co. v. Gulf Oil Corp*, 541 F.2d 1263,1266 (7th Cir. 1976), provide that the "the party not suffering the force majeure *may terminate* and neither party shall have further obligation

to the other with respect to fuel not yet delivered." (Emphasis added) In other cases, like *Princeton Cmty.*, mere suspension of the contractual obligation is triggered. In the case of a terminable force majeure event, the terminating party can attempt to escape arbitration all together. This can avoid the arbitration forum.

Identification issues

The clause in *Princeton Cmty.* limited force majeure to "government acts." As a result, a private cyberattack would not be covered. But even where identification of the hacker is legally relevant, this determination source is often quite difficult. In some cases, "false flag" strategies may be used to camouflage the real source of the attack. A private actor can camouflage itself under the guise of a state actor.

Clause suggestions

Tech contracts like software licenes can – and should -- include force majeure clauses. Drafting the clause to make sure that mere suspension – and not termination – of obligations is essential. Otherwise, like in *Commonwealth Edison*, the party not suffering the event can seek terminate when there is a cyber-attack. Defining "force majeure" to include cyber-attacks regardless of their source – even private ones, as long as they are significant -- is another way to avoid this issue of identification all together.

Conclusion

Cyberattacks are increasingly common. Ensuring they are carefully dealt with in agreements – especially for software -- is even more important. This can prevent parties from trying to avoid arbitration. Whether adequate measures were taken to prevent the cyberattack, to make it unforeseeable, is something beyond the scope of this article.

Ryan is a Santa Monica based tech / media attorney and a Stanford Law School Center for Internet and Society non-residential fellow. He has over 15 years of experience solving tricky intellectual property issues for pioneering clients including former Google privacy researcher Dr. Martin Shelton and Taiwan based hardware company LegendSky Tech Co. Ltd. He has written for or been interviewed by the likes of *Cognitive Times* and *Digital Trends* about new tech subjects such as facial recognition technology and "deep fake" videos, respectively.