THOMPSON HINE

Privacy & Cybersecurity Update

July 19, 2024

The Microsoft Outage, Cyber Disruptions, and Force Majeure Events

Recent media reports indicate that many organizations, across a range of business sectors (e.g., banks, airports, hotels) are facing widespread information technology (IT) outages due to a disruption impacting Microsoft operating systems. According to the reports, the IT outages are the result of supply chain "updates" and not a cyberattack. This incident serves as an important reminder for organizations to assess how their customer and supply chain contracts address force majeure events arising from upstream IT and other cyber disruptions, especially in light of how major cybersecurity events could impact their ability to fulfill obligations under their business contracts, whether or not the underlying cause of these outages was malicious.

Contract Drafting and Similar Considerations

A force majeure clause is a contract provision or term that provides for a defense to liability or otherwise allocates the risk of loss among the parties if performance of a contractual obligation is delayed or becomes impossible or impracticable, especially as a result of an event or effect the parties could not have anticipated or controlled. The scope and application of a force majeure clause depends on the specific terms of the contract in question. The fact that a contract contains a force majeure clause does not necessarily mean that a party has the right to invoke relief as a result of impacts to its business resulting from a ransomware attack, business email compromise, or other IT disruption. Rather, the parties will need to determine whether a force majeure event has occurred under the terms of the contract.

A force majeure clause is generally drafted to identify specific types of events that may excuse performance and usually requires the event to be beyond the parties' "reasonable control." In some cases, it also requires that the event was not reasonably foreseeable. Traditionally, these events have included acts of God, labor shortages or strikes, governmental orders or regulations, fires, and environmental disasters, and in recent times they have been expanded to include pandemics, nuclear incidents, riots, wars, and terrorism.

However, in light of major cybersecurity events in recent years, it is becoming more common for force majeure events to be defined to expressly include:

- Denial of service attacks
- Ransomware or similar intrusions into critical IT systems and networks
- Service disruptions involving key hardware, software, or IT systems not within the party's possession or reasonable control
- Electrical, internet, or telecommunications outages that are not caused by the obligated party

A favorable force majeure clause may be so expansive as to include supply delays, material shortages, or increased costs or delays in obtaining goods, workers or transportation.

Interpretations of force majeure provisions can vary greatly across states and even more so in foreign (non-U.S.) jurisdictions. Accordingly, the choice of law provision in the contract is key to its interpretation and will establish what jurisdiction's law governs. Each U.S. state except Louisiana has enacted some version of the Uniform Commercial Code (UCC), though they are not all identical. In addition, not all state and federal courts interpret the UCC provisions in the same manner. In the case of international commerce, the United Nations Convention on Contracts for the International Sale of Goods applies unless it is specifically disclaimed in the contract.

A force majeure provision should also impose protocols for notice, timetables for non-excuse or termination, and other terms relevant to evaluating a force majeure declaration and the way it is made. If applicable, a party's compliance with these protocols can impact whether the declaration is valid and if performance can be excused.

Important Precedent in the Cyber Context

There are only a few judicial decisions addressing whether large-scale cybersecurity events, like ransomware attacks, are considered beyond a party's "reasonable control" for the purpose of interpreting a force majeure clause. The two leading cases in this area both relate to the Russian military-launched NotPetya cyberattack in June 2017.

Princeton Cmty. Hosp. Ass'n v. Nuance Communs., Inc., No. 1:19-00265, 2020 U.S. Dist. LEXIS 60490 (S.D. W. Va. Apr. 6, 2020), involves civil litigation arising from the NotPetya cyber operations. Here, the plaintiff (Princeton Community Hospital Association, Inc.) alleged that software from the defendant (Nuance Communications, Inc.) was integrated into its hospital computer network, which was corrupted during the NotPetya event, resulting in the plaintiff's IT systems being "infected by malicious malware that embedded and destroyed" all data and encrypted its "entire computer health network." The plaintiff argued that the defendant was responsible for its total damages in the amount of approximately $6.8 million. The master agreement between the two parties included a force majeure clause that the defendant wanted to invoke to excuse itself from liability. The defendant contended that the malware attack clearly fit within the language of the force majeure clause that excused the defendant's "nonperformance." The court assumed – but did not decide – that the NotPetya attack was a "governmental act or order," "act of terrorism," and/or "act of war."

Heritage Valley Health Sys. v. Nuance Communs.", Inc., 479 F. Supp. 3d 175 (W.D. Pa. 2020), sets forth a similar set of circumstances. Here, the plaintiff (Heritage Valley) claimed that it suffered damages when malware from the NetPetya cyberattack entered its computer network system through a network connection with the defendant (Nuance Communications, Inc). The plaintiff alleged that the attack's success was a result of the defendant's "poor 'security practices and governance oversight'" and "of [the defendant's] own information security failings." The agreement between the plaintiff and defendant included a force majeure clause. While the defendant's motion to dismiss was granted due to other defenses, the court noted in a footnote that "a cyber-attack launched by the Russian government which affected many other companies and organizations worldwide – was arguably beyond [the defendant's] reasonable control."

Conclusion

A force majeure clause is a bargained-for assumption of risk provision and is becoming more important in contract negotiations. In light of major disruptions to contractual performance obligations in recent years (e.g., COVID-19, global cyberattacks), these clauses can no longer be viewed as boilerplate or an afterthought. The recent Microsoft incident serves as an important reminder for organizations to assess how their customer and supply chain contracts address force majeure events arising from IT and other cyber disruptions.

FOR MORE INFORMATION

For more information, please contact:

Steven G. Stransky
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)

Jennifer N. Elleman
937.443.6927
Jennifer.Elleman@ThompsonHine.com

John D. Cottingham
513.352.6674
John.Cottingham@ThompsonHine.com