Professional Perspective

Force Majeure, Privacy and Cybersecurity

Eric Hess, Hess Legal Counsel

Bloomberg
Law

Read Professional Perspectives | Become a Contributor

Force Majeure, Privacy and Cybersecurity

Contributed by Eric Hess, Hess Legal Counsel

Introduction

Early in 2020, the Covid-19 pandemic sent contract lawyers scrambling to understand the largely boilerplate force majeure clauses governing their contracts. Rightfully so, as force majeure can allow parties to suspend all or part of contract performance if certain defined unforeseeable events occur. The renewed attention on these clauses prompted the International Chamber of Commerce to offer balanced templates early last year, as well as numerous law firms to publish their analyses.

Force majeure clauses, however, were undergoing an evolution with regards to technology and security events well before the pandemic. Drawn from the Napoleonic Code of 1904, common law has no concept of force majeure and it is enforced according to its terms. Thus, specific cyber security attacks like DDoS (distributed denial of service), advance persistent threat (APT), and ransomware have been added by lawyers to the list of triggering events, as well as technology failures relating to telecommunications, systems, network, software, power and even hardware. These inclusions, however, can conflict with other contractual protections specifically covering such attacks and failures.

In early December 2019, FireEye discovered that a threat actor had compromised Solar Winds' network monitoring program used by multiple federal agencies, including the U.S. Treasury, Homeland Security, Department of State, Department of Energy and National Nuclear Security Administration, and a hundred technology companies. The scope of this attack is still being investigated and the Biden administration recently announced that they would be taking executive action to address the security shortcomings that this attack has uncovered. What the SolarWinds attack demonstrates is that no organization is immune from cybersecurity compromises and underscores the need for lawyers to, once again, contemplate applicable force majeure clauses, particularly with regards to the processing or storage of personal identifiable information given evolving privacy regulations. In doing so, counsel needs to carefully contemplate the appropriate definition of force majeure events, alignment between such events and intended allocation of risk, alternatives to suspension and the force majeure event lifecycle.

Defining and Aligning the Force Majeure Triggering Events

Given its absence from common law, jurisdictions will generally interpret force majeure events narrowly. In re Cablevision Consumer Lit., New York's Eastern District found that force majeure "will generally only excuse a party's nonperformance if the event that caused the party's nonperformance is specifically identified." As noted above, the laundry list of failures and attacks may conflict with the expectations of the parties with regards to redundancy, high availability, disaster recovery and service level terms. Similarly, exclusions for cybersecurity breaches may conflict with a variety of representations, warranties, covenants and service levels related to security. The interaction of such contractual terms, as well as other self-help rights, such as step in or emergency IP licensing, with force majeure should be contemplated as part of the contractual process.

Sometimes vendor counsel will insert supplier and subcontractor delays as an event of force majeure which could have the unintended consequences of causing non force majeure events, such as a contractual dispute between the vendor and the fourth party provider, to rise to the level of force majeure between the vendor and its customer on the other side. From a customer perspective, if permitted, such delays should be limited to declared force majeure events, thus embedding fourth party force majeure into third party force majeure clauses.

The mere occurrence of these events is not enough to invoke a force majeure claim. A force majeure event generally requires the satisfaction of three criteria:

- It must be beyond the affected party's reasonable control.
- The affected party's ability to perform under the contract must have been prevented, impeded or hindered by it.

- The affected party must have taken all reasonable steps to seek to avoid or mitigate the event or its consequences.

Mitigation and Remediation

Counsel must consider how enumerated events and triggering criteria align with the protective and remedial expectations of the parties regarding an attack or technology related failure. For example, a customer's expectation that a vendor has invoked its business continuity or disaster recovery procedures before declaring an event of force majeure should be made explicit, as well as a statement that vendor's execution of such procedures shall not be subject to suspension. Additionally, a suspension of a vendor's security obligations, particularly where personal identifiable information is involved, could have a domino effect across customer contracts, create regulatory exposure and require disclosures.

In such cases, the applicability of cybersecurity and privacy regulations should be noted in the force majeure clause provision. Counsel may also need to consider a more limited suspension of contractual obligations so that critical regulatory, security, business continuity, and reporting obligation performance is not impacted during the pendency of a force majeure event.

To further complicate matters, even where applicability of such regulations has been contemplated by the parties, privacy regulations continue to evolve, with more states likely to follow the lead of California. The result is that what may have been a contractual obligation between the parties, has emerged as a regulatory requirement with consequences for both the vendor and the customer. Indeed, this could be a larger contractual issue.

The proper approach here is, where personal identifiable information is being processed or stored, force majeure needs to contemplate cooperation on the parties' regulatory and data security obligations. The International Association of Privacy Professionals (IAPP) published a guide tracking state by state adoption of privacy laws, but European Union data regulation, including the General Data Protection Regulation, and other applicable international regulation must also be contemplated where the data of international residents is implicated. Arguably the appropriate standard should be the privacy regulations of the most stringent applicable jurisdiction. The impact on the regulatory obligations respecting such data should be contemplated across individual rights of access, rectification, deletion, restriction, portability, opt-out, automated decision making, sale of information, data breach notification, purpose and processing limitations, and fiduciary duty.

Practitioners should also consider impacts of a force majeure event on security certifications, such as a System and Organization Controls (SOC) report, or written security and privacy attestations, as force majeure could render those certifications or attestations stale and inaccurate. Counsel for the customer must contemplate the impact of such a breach, as well as notification, mitigation or remediation measures that might be required to be undertaken as a consequence.

Initiation and Pendency of a Force Majeure Event

The inclusion of cyber-attacks or technology failures as force majeure events may implicate each party's cybersecurity and privacy responses. Vendor counsel should contemplate the vendor's possible need to engage counsel and conduct a preliminary forensics examination, particularly if cybersecurity breach notification laws are triggered. Counsel engaged post breach may desire to curb certain disclosures. Anything more than ten business days from the date of the force majeure triggering event would generally be considered off market. On the customer side, counsel should contemplate the need for the customer to undertake their own mitigation actions, as well as engaging their own counsel and forensics examination. Further, the need for the vendor to provide continuous updates should be contemplated. The parties' obligation to cooperate with any forensics examination should continue during the pendency of force majeure suspension.

Termination and Transition

While most force majeure clauses allow for termination of a contract if the force majeure event occurs for a specified period, technology contracts may present greater transitional issues for the customer. Counsel may require a vendor's transitional assistance to prepare for a possible termination and thus waiting in limbo prior to the termination date may not suffice. A customer may require vendor transition assistance to prepare for the possibility of termination.

Customer counsel may also seek a review of the vendor's business continuity procedures to understand what processes would accommodate such a transition since simply negotiating in an obligation may be less meaningful then ensuring that the parties understand how that transition assistance would actually be executed.

Conclusion

In reviewing the above considerations, the risks and practicality of permitting force majeure suspensions of specific cybersecurity and privacy obligations needs to be considered, as well as evolving privacy regulations. Appropriate risk allocation for force majeure events may be better contemplated as part of other contractual provisions, such as limitations of liability and covenants, so that outcomes are more aligned for both vendors and their customers.