MILLER CANFIELD

Preparing for Cyberattacks and Limiting Liability

February 28, 2022

The U.S. government and military experts have been warning U.S. companies that Russia may launch significant cyberattacks against critical infrastructure, financial institutions and businesses in retaliation for the sanctions imposed against Russia. Last week, the Cybersecurity & Infrastructure Security Agency (established in 2018 under the Department of Homeland Security) made available on its **website** free services and tools for U.S. companies to enhance their cybersecurity risk management capabilities. Now is the time for companies to ensure that they undertake a comprehensive risk assessment and implement the necessary cybersecurity measures to mitigate potential liability in the event of a cyberattack.

The Legal Landscape

A cyberattack exposes a company to two major legal risks. First, if the cyberattack causes a significant disruption, shutdown or delay in performance, a company may not be protected from liability with a contractual force majeure clause or other theory of law. Second, depending on the scope and type of data impacted, there may be liability under data privacy laws and regulations.

Force Majeure and Other Theories of Law

If a company experiences a cyberattack that disrupts its business operations, force majeure clauses and the other statutory and common law doctrines to excuse performance may offer little or no protection to the company in a lawsuit unless the company can show that it took all reasonable actions to try to prevent the cyberattack from disrupting its business.

A company should not assume that a cyberattack from a foreign agent would be excusable as a force majeure event. Whether or not a cyberattack could constitute a force majeure event would depend on the language of the specific contract between the company and its counterparty. Most force majeure clauses do not include any reference to a cyberattack, sabotage, terrorism or computer hack. But even if such an event is included, it is usually qualified by the requirement that the event be beyond the "reasonable control" of the affected party, which may require the party to prove that it took reasonable measures to prevent such an attack from disrupting its business operations.

More typically, force majeure clauses are written broadly to include a "catch-all" or any event beyond a party's "reasonable control." However, the courts of many jurisdictions interpret force majeure catch-all clauses narrowly, so a court may decide that a cyberattack is not covered under a force majeure catch-all clause.

As an alternative to a contractual force majeure clause, statutory and common law doctrines of commercial impracticability, impossibility and frustration of purpose might be invoked to excuse performance after a cyberattack. However, in general, courts also construe these doctrines narrowly and take into account factors such as foreseeability, reasonable control, and the preventative actions that were or were not undertaken by the party.

In essence, force majeure and the other statutory and common law doctrines to excuse performance in the event of a cyberattack generally have limited applicability, but in any case, as a prerequisite, the company will need to show that it took all reasonable actions to try to prevent the cyberattack from disrupting its business operations, including, specifically, adopting and implementing a cybersecurity plan.

Data Privacy Laws and Regulations

A variety of federal and state laws, regulations and industry standards require companies to implement measures to secure personal and other information. The below list highlights laws that directly address data breaches. However, this is not an exhaustive list, and lawmakers or regulators may step in if a cyberattack affects consumers or market participants:

- FTC Act (prohibits unfair or deceptive commercial practices, including failing to provide reasonable and appropriate security measures for sensitive consumer information)
- HIPAA (includes the Standards for Privacy of Individually Identifiable Health Information, which applies to the collection, use and disclosure of protected health information, and regulates the use, disclosure, maintenance or transmission of such information)
- ERISA (cybersecurity breaches and fraudulent distributions involving retirement plans and participant information and data may constitute a breach of the fiduciary duty of plan sponsors and service providers)
- California Consumer Privacy Act of 2018 (CCPA) (requires reasonable information security practices and data breach notification)
- Massachusetts Data Security Regulation (requires companies to develop, implement and maintain a comprehensive, written information security program that addresses specified safeguards)
- Payment Card Industry Data Security Standard (PCI DSS) (requires all entities that process, store, or transmit cardholder data to comply with certain security requirements)
- ISO 27001 (provides a security framework created by the International Organization for Standardization that assesses a company's ability to keep its data safe)

To the extent a cyberattack results in a data breach or disclosure of protected personal information, the company may face not only statutory or regulatory penalties and fines but also lawsuits from impacted consumers. Additionally, commercial customers or suppliers may claim breach of contract because many commercial contracts obligate parties to safeguard data and information and to adhere to ISO 27001 or similar industry standards.

Implementing a Cybersecurity Plan

It is imperative for a company to make reasonable efforts to keep its data and personal information secure. Fundamental to that effort is for the company to adopt and implement a written cybersecurity policy and plan, setting forth company cybersecurity policies to prevent data breaches and procedures detailing the appropriate responses and actions to be taken in the event of a cyberattack.

As an initial step, it is generally recommended that each company appoint a team dedicated to the company's cybersecurity plan. The team should be responsible for developing the written cybersecurity policies and response plan, as well as for investigating cyberattacks and attempts in accordance with that plan. The cybersecurity plan should generally address these basic components:

Safeguarding Data

- Create barriers to cyberattacks (e.g., require employees to change passwords every 90 days)
- Create document retention and disposal policies to ensure that employees are keeping the right records
- Set employee expectations (e.g., no posting sensitive information on social media)
- Understand what data is going to and coming from third parties including customers and vendors to make sure that the proper checks are in place

Training, Training, Training

For a company's cybersecurity plan to be meaningful and effective, the company's workforce, including executives, employees, and contractors, must participate in detailed and frequent training and educational programs. Cybersecurity programs should include courses on regulatory compliance, information classification, personnel security and access management, acceptable use, computer and data security, incident response, service provider oversight, and risk and compliance management. Legal counsel should customize the training modules to fit the company's specific cybersecurity policy and legal obligations.

Reporting a Cyberthreat and Cyberattack

Each company employee should know whom to contact to report potential incidents, whether it be a supervisor or the company's cybersecurity team and/or IT representatives. The company's management, board of directors or other governing body should be kept informed of any cybersecurity incidents and thwarted threats.

Importantly, statutes, regulations and even contractual provisions may require notifying customers, regulators and affected persons. Not all cyber threats warrant disclosure or external communication. Any notifications need to be handled in a timely manner with a coordinated message among the company's management team, legal counsel, and communications team.

Cyber Insurance

Another potentially useful tool for a company to consider including as a part of its cybersecurity plan is cyber insurance. Cyber insurance generally covers a company's liability for data breaches involving sensitive customer information. More and more companies are also contractually requiring that their vendors carry their own cyber insurance to cover the company's data which is in the possession of their vendors.

Cyber insurance can include first party coverage, which covers the costs incurred by the insured in connection with implementing a plan, training employees, undertaking security assessments, as well as the costs incurred in the event of a data breach, such as hiring attorneys, computer forensic firms, notifying affected persons of the breach, etc. Cyber insurance can also include third party coverage, which covers the insured from liability to third parties resulting from the data breach, such as fines, litigation defense costs and damages.

A company's general liability insurance policies also need to be reviewed, as some general liability policies may already cover some of the risks of cyberattacks. Cyber insurance policies can be complex and difficult to decipher, so legal counsel should be consulted.

Continued

Please contact the authors to further discuss these developments.