Proskauer

Held to Ransom: How Cyberattacks Can Become a Legal and Regulatory Odyssey for a Private Investment Fund - Part 2

Cybersecurity Law Report on **October 19, 2022**

Imagine this: You work for a private investment fund manager. It is Monday evening. The finance director of one of the fund's portfolio companies, a well-known payment services provider, calls. The company has discovered ransomware barring it from accessing the majority of its IT systems and the cyber threat actors are demanding a ransom before they will hand over the decryption key. The ransom will double each day it remains unpaid, and if the company does not pay, the attackers will publish all of the personal information and sensitive business information they have captured. Within two days the ransom will exceed the company's cyber insurance coverage and it will need a cash injection from the investment fund to satisfy the ransom demand. What do you do?

Part one of this series set out the issues to keep in mind in terms of immediate incident response and weighing whether to pay the ransom. This second installment reviews the regulatory obligations that arise on any data breach and considers the follow-on steps and consequences of such a breach from both a U.S. and U.K. perspective.

Related Professionals

- **Margaret A. Dale**
  Partner
- **Dorothy Murray**
  Partner
- **Todd J. Ohlms**
  Partner
- **Jonathan M. Weiss**
  Partner