Proskauer

Held to Ransom: How Cyberattacks Can Become a Legal and Regulatory Odyssey for a Private Investment Fund - Part 1

Cybersecurity Law Report on **September 21, 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 hackers 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?

Where business-critical information or platforms are at stake, many commercial parties will seriously consider immediately paying the ransom hoping to regain control of operations, secure client data and avoid continued business disruption and negative publicity. However, businesses may wish to pause. Cyberattacks, by their very nature, know no borders and nor therefore should a private fund's response. In the first of this two-part series for *Cybersecurity Law Report*, partners Ryan P. Blaney, Margaret A. Dale, Dorothy Murray, Todd J. Ohlms and Jonathan M. Weiss outline immediate incident response steps and analyses whether to pay a ransom, from U.S., U.K. and E.U. perspectives.

Related Professionals

- **Margaret A. Dale**
  Partner
- **Dorothy Murray**
  Partner

- **Todd J. Ohlms**
  Partner
- **Jonathan M. Weiss**
  Partner
- **Seetha Ramachandran**
  Partner
- **Kelly M. McMullon**
  Special International Labor, Employment & Data Protection Counsel