Proskauer

Private Equity and Cybersecurity: A Guide to Preparing for and Responding to a Breach

The Capital Commitment Blog on **September 15, 2020**

A cyber breach can have serious legal, financial, and reputational consequences for a fund sponsor, as described in our previous post. As such, cybersecurity threats must be treated as business risks, not just a potential IT problem. Senior management at fund sponsors should take the lead to ensure that the sponsor is taking appropriate actions to protect itself against cyber risks. There are several steps that senior management can guide the fund sponsor to take to prevent breaches from occurring and to mitigate the impact when they do occur.

Be Prepared

Careful planning and preparation, including appropriate policies and procedures, is critical for the creation of an effective cybersecurity program. The program should include a Cyber Risk Assessment and a Cyber Incident Response Plan.

Perform a Cyber Risk Assessment

- Information: Identify the information and data that is most sensitive and important to the sponsor. Commentators often refer to this as the "crown jewels." This will often include information about finances or personally identifying information ("PII"). PII can include individuals' names, addresses, social security numbers, and other sensitive information about a person.
- Resources: Devote appropriate staff for the supervision and oversight of cybersecurity measures on an ongoing basis, including having personnel responsible for staying up-to-date on evolving threats, and maintaining all cybersecurity related reports and information.
- Compliance: Ensure compliance policies satisfy fund governance agreements.
- Ensure vendor compliance: Review the cyber risk protocols of any vendors who may have access to sponsor data. In particular, the SEC has been especially focused on third party service providers that may have custody of, or access to, PII.

- Test: Stress test the relevant computer networks in order to identify and assess vulnerabilities.
- Implement prophylactic measures: Regularly backup important data to guard against ransomware attacks. If the victim has backup copies, the hacker no longer holds the upper hand. Registered investment advisers should already be taking steps to protect, backup and preserve their books and records and customer information pursuant to Rule 204-2 of the Investment Advisers Act and Rule 30 of Regulation S-P.
- Audit: Institute recurrent security audits to identify potential risks.

Cyber risk assessment is an ongoing process that should be continually revisited and revised to account for the changing regulatory landscape and technological advances.

Adopt a Cyber Incident Response Plan

Assign a “quarterback” to lead response efforts, including coordinating mitigation efforts, remediation actions, and possible law enforcement referral.
Coordinate with outside counsel who can act quickly if a breach does occur, and who can coordinate other professionals, such as forensic and IT professionals, while working to protect information through the assertion of privilege.

- Outline a plan for coordinating with regulators and law enforcement agents.
- Evaluate the potential need to communicate with investors in the sponsor’s funds in the event of a breach.
- Retain a public relations consultant to monitor social media and news reports regarding the sponsor and its funds after a breach for the purpose of brand protection.

Counsel should assist with these tasks to ensure that the fund sponsor is prepared and protected.

Follow the Plan

An effective Cyber Incident Response Plan should provide a roadmap for the sponsor in the event of a breach. Speed is crucial when responding to a breach, particularly in the first twenty-four hours, to try to minimize the impact.

- Contact counsel identified in the Cyber Incident Response Plan, to engage relevant professionals including, among others, an IT provider and/or a forensic investigator.

- Define the scope of the breach and assess what systems and data have been compromised. Determine if a backup of any lost data is available.
- Consider whether notice to law enforcement and/or regulators is necessary or appropriate.
- Assess with counsel whether the breach has triggered notification requirements to fund investors or others under any applicable laws or contracts.
- Evaluate with counsel potential insurance coverage, along with regulatory and/or civil litigation risks.

If questions arise concerning the risk-reduction measures outlined above, we are available to consult as needed.

View Original

Related Professionals

- **Margaret A. Dale**
  Partner