Cybersecurity Law Report cslawreport.com

Feb. 1, 2023

Due Diligence

Data Breaches and the Private Credit Market: Assessing Borrower Cyber Preparedness

By Ryan Blaney, Bharat Moudgil and Evan Palenschat, *Proskauer*

Hackers seeking access to confidential material and personal information about clients, partners, investors and employees have proved to be costly and dangerous for business owners. Given the material costs and reputational harm associated with a data breach, lenders should remain vigilant for potential cybersecurity-related pitfalls in their credit documents. Understanding how to assess companies' vulnerabilities and how to address them during diligence and documentation will help them maintain a constructive partnership with their borrowers in the event of an incident and arm them with knowledge necessary for a fulsome underwriting process.

Healthcare, software and technology, and business services were the three leading borrower industries represented in the over 400 financings Proskauer's private credit group closed in 2021, comprising half of the transactions. Given the amount of capital flowing into these spaces, lenders need to be aware of the costs and risks associated with cybersecurity incidents, and also what steps can be taken to protect their credit.

In this first part of a two-part article series, we discuss the cost of breaches, why vigilance is urgent and proactive steps to take to assess a borrower's preparedness. Part two will cover how to prepare for and address a borrower's breach.

See "Identifying and Tackling Privacy and Cyber Due Diligence Challenges in M&A" (Mar. 23, 2022).

By the Numbers: How Much a Data Breach Costs and Why It Should Matter to Lenders

Between 2020 and 2022, the average total cost of a data breach increased by over 12%, from $3.86 million to $4.35 million. In the United States the cost of a breach is even higher, with average costs at $9.44 million. The COVID-19 pandemic played a large part in the year-over-year jump. As businesses scrambled to launch or enhance their remote working infrastructure, the associated costs of a data breach increased by approximately $1 million where remote work was a factor in the underlying breach.

Remote work not only increased the cost associated with a data breach, but it limited organizations' ability to act as quickly in response to the underlying issues. Companies with more than 50% of their workforce working remotely took nearly 60 days longer to identify and address breaches as compared with companies with less than half their workforce at home. As industries grapple with potentially long-term hybrid working environments, these issues will persist.

The costs associated with a data breach can take many forms, but lost business costs lead the way: in the 2020-2021 period, lost business constituted nearly 40% of breach costs, including customer turnover, revenue losses and reputational harm. These costs multiplied in so-called "mega breaches," which are breaches involving more than one million records. On the high end, these incidents resulted in an organizational cost of nearly $400 million.

More than 700 direct lending funds provided private debt at the end of 2021, according to the 2022 Preqin Global Private Debt Report. As global private debt assets under management continue to grow – they are projected to reach over $2.6 trillion by 2026 – effective lender response to the increasing risk of cyber incidents will receive additional scrutiny from underwriters.

Assessing a Borrower's Preparedness

Careful planning and preparation of a cybersecurity program, including appropriate written policies and procedures, is critical for effective breach response, and lenders should be aware of how to assess for an adequate set of defenses when engaging in diligence on a potential borrower. A company's program should, at a minimum, include a cyber risk assessment and a cyber incident response plan. While there will be common elements among different organizations, there is no replacement for a program that is tailored to the company's business and has been exercised regularly.

See How to Conduct Effective Privacy and Data Security Diligence to Assure Value Realization in Mergers, Acquisitions and Divestitures" (Oct. 27, 2021).

Cyber Risk Assessments

A cyber risk assessment is an ongoing process that should be continually re-evaluated to account for the changing regulatory landscape and technological advances. The borrower should be conducting assessments at regular intervals and incorporating them into the company's written cybersecurity policies. The assessment should identify the information and data that is most sensitive and important to the company. 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.

The assessment should review the cyber risk protocols of any vendors who may have access to company data. The SEC has been especially focused on third-party service providers that may have custody of, or access to, PII. Regular third-party audits of information systems have become standard for businesses handling PII.

See Cybersecurity Law Report's two-part series on SEC cyber rules: "How to Prepare for the New 8-K Incident Mandate" (Aug. 10, 2022); and "How to Prepare for the New 10-K Disclosure Mandates" (Aug. 17, 2022).

Privacy Policies and Data Security Measures

Lenders and their counsel should assess the scope of a borrower's privacy policy and historical compliance with privacy laws. They should also examine the strength of a borrower's existing data security measures and get as much information as possible with respect to past incidents and what institutional changes were made to prevent repeat occurrences.

If, for example, the company has a history of cybersecurity litigation, the lender could then cap the amount of litigation expenses that can be added back to EBITDA, which is a metric for the company's financial health and a component of calculating its leverage profile.

Incident Response Plan

The borrower should have an effective incident response plan, which provides a roadmap for the company in the event of a breach. Speed is crucial when responding to a breach, particularly in the first 24 hours, to try to minimize the impact, and the lender should ensure the borrower's plan provides for swift action.

If the plan is lacking, consider requiring borrowers to update their cyber incident response plans so that they have a robust and actionable trouble-shooting plan in the event of a data breach.

See "How to Establish an Efficient Incident Response Plan" (Jul. 17, 2019).

Officer In Charge

A company's incident response plan should identify the officer who is tasked with leading response efforts, including coordinating mitigation efforts, remediation actions and possible law enforcement communications. That officer will be the main point of contact with the company's senior management and with outside counsel, who can act quickly if a breach does occur and engage relevant professionals including, among others, an IT provider and/or a forensic investigator while working to protect information through the assertion of privilege.

The technical professionals will work with the company to determine the scope of the breach and assess what systems and data have been compromised.

Notification

Notification provisions should also be part of the plan. The scope of the breach will determine whether notice to law enforcement and/or regulators is necessary or appropriate, and the lenders should expect that legal counsel should be involved in all communications with regulators and the af-

fected individuals. The breach may also trigger notification requirements to customers[1] or others under commercial agreements, including a lender's credit agreement if that was negotiated during the documentation phase, as more fully discussed below.

Communication

The borrower's incident response plan must address the potential need to communicate with investors, lenders or customers in the event of a breach. Certain organizations choose to retain a public relations consultant to monitor social media and news reports regarding the company after a breach for the purpose of brand protection. This should be of particular interest to lenders who will be concerned about any reputational impact to the borrower and any corresponding financial effects to the borrower's business that could ultimately lead to a default under its credit agreement.

See "Incident Response in the Financial Services Industry" (Jul. 28, 2021).

Third-Party Contracts

A careful analysis of the company's commercial contracts will help mitigate the risk of breach in those agreements and that should be a point of focus for the company and its lenders. If the company has cyber insurance coverage or is required to maintain it pursuant to a credit agreement, the policy should be reviewed with counsel together with a discussion about the regulatory and/or civil litigation risks.

Insurance Policy

Check for cyber insurance. Maintaining a specific cyber insurance policy has become standard for any company operating with consumer data or transacting on the internet. Policies vary greatly, and it is important to understand the different risk areas when choosing a policy.

Losses following a data privacy or cybersecurity event could include lawsuits from affected individuals, fines from a regulator, breach of contract claims from a business partner, cost of notifying affected individuals, ransom paid to malicious actors, physical damage to equipment, losses due to system downtime, costs repairing and improving software systems, and third-party consultants, technicians and counsel.

Cyber insurance policies will cover some combination of these losses, and it is important for a lender and its legal counsel to analyze which losses a borrower's business may be particularly sensitive to in the diligence process and ensure that such losses are covered by the underlying insurance policies. Following a data privacy event, as discussed in the next part of this two-part series, looking to the borrower's cyber insurance policy should be among the very first steps to ensure that the borrower's response is compliant with the policy's terms.

Unless the company is in an industry prone to data breaches or in one that has historically been subject to data breach incidents, the company may not have obtained a cybersecurity policy prior to the

breach. General liability insurance may not cover liabilities associated with data breaches.

Lenders could explicitly require a borrower to maintain a cybersecurity insurance policy, particularly in businesses that operate in vulnerable industries. Most lender documents will require that a borrower maintain insurance reasonably equivalent to similarly situated borrowers in the same industry.

See "Cyber Insurance Litigation Trends Amid Rising Ransomware Attacks" (Nov. 10, 2021).

Ryan P. Blaney is the head of Proskauer's global privacy and cybersecurity group. He is based in Washington, D.C.

Bharat Moudgil is a partner in the firm's private credit group and is based in Los Angeles.

Evan Palenschat is a partner in the firm's private credit group and is based in Chicago.

[1] *See e.g.*, Cal. Civ. Code § 1748.12(b); Conn. Gen. Stat. § 36a-701b; Colo. Rev. Stat. § 6-1-716; New York General Business Code 899-aa.