THOMSON REUTERS
PRACTICAL LAW™

Expert Q&A on Cyber Risk in Finance

by Robert Blamires, Tony Kim, and Jane Summers, Latham & Watkins LLP with Practical Law Finance

Status: **Published on 02 Mar 2022** | Jurisdiction: **United States**

This document is published by Practical Law and can be found at: **us.practicallaw.tr.com/w-034-4295**
Request a free trial and demonstration at: **us.practicallaw.tr.com/about/freetrial**

An expert Q&A with Robert Blamires, Tony Kim, and Jane Summers, Latham & Watkins LLP, on cyber risk in finance transactions. This article includes a discussion of how the evolution of cybersecurity-related representations and warranties in M&A transaction documentation has had an effect on finance deals.

What is the Current Cybersecurity Threat Landscape That Companies Face?

We see three unmistakable trends:

- First, threat actors are increasingly sophisticated in their use of tactics, techniques, and protocols designed to circumvent security controls, to avoid detection, and even to obfuscate or remove forensic evidence (for example, logs). Look no further than recent, high profile cyberattacks that have:
  - specifically targeted companies on the eve of major M&A transactions or IPOs to maximize leverage for extortion payments; or
  - infiltrated the supply chain to affect thousands or even tens of thousands of companies.
- Second, there is an increasing use of double-extortion ransomware attacks, in particular, two-part attacks that combine data exfiltration and corresponding disclosure threats with disabling systems and encrypting data, followed by demands for ransom payments (typically in hard-to-trace cryptocurrencies).
- Third, the accelerated attack activity has put regulators and plaintiffs into over-drive. As just one example, the US Treasury's Office of Foreign Assets Control (OFAC) issued an advisory in late 2021 warning that not only victim companies, but any third parties (for example, payment processors, forensic investigators, insurance carriers) involved in facilitating payments to sanctioned ransomware actors, were fair game for enforcement (for more information, see Legal Update, OFAC Issues Guidance and Updated FAQs on Virtual Currency Sanctions Compliance and FinCEN Issues Updated Advisory on Ransomware). To cap things off, it appears that the cyber insurance marketplace is shrinking the scope of available coverage for incidents like ransomware.

What are the Most Pressing Cybersecurity Risks in the Deal Market and How Do They Impact Borrowers and Lenders?

Cyber risk is always evolving, but fundamentally it should factor into a deal just like the risk of data privacy breaches and non-data specific concerns (environmental, litigation, intellectual property, tax, benefits, and the like). With respect to risk generally, parties conduct diligence and negotiate to arrive at appropriate ways to assess it, to allocate it, and to arrive at terms that reflect these assessments and the allocation of attendant risk.

The critical cyber-related questions to answer are whether cyber threats pose existential risk to the borrower or, even if not existential, could affect the borrower's ability to service debt, the borrower's stock price, the borrower's ability to retain customers and operations, or could lead to material downstream liability (for example, investigations, litigation, customer issues, or brand or reputational impact). These risks tend to be greater in the context of borrowers who have experienced one or more cyberattacks or other security incidents, especially when the incident occurs during the transaction itself, which we are seeing more and more often.

What Diligence Can Borrowers and Lenders Undertake to Address Cyber Risks?

Standard diligence involves document review, management interviews and analysis of publicly available information

and materials. That standard level of diligence is likely to remain the baseline. From there, the scope of any given diligence exercise will be context-specific and aligned to the cybersecurity risk profile of the borrower (including what data they hold), the borrower's industry, and the surrounding regulatory and litigation climate.

A key issue also revolves around whether the borrower has suffered a recent cyberattack. If so:

- What was the impact of the cyberattack (if any) on the borrower's network, systems, proprietary and confidential data (for example, personal information), operations, forecasted business relationships, reputation, business valuation and the like?
- Was the borrower able to recover effectively and efficiently?
- What information security program gaps did the incident investigation uncover?
- Does remediation appear to have addressed any identified cyber vulnerabilities and program gaps on a go-forward basis?
- Did or will any regulatory investigations or lawsuits follow?

How Have Cybersecurity Representations and Warranties Evolved in M&A Transaction Documents and How Have They Affected Financing Terms?

Historically, cybersecurity (like data privacy) was captured within "comply with all applicable laws"-type boilerplate provisions. However, the legal compliance regime governing implementation of security measures has been and remains relatively undeveloped. In addition, over time, as non-security folks (for example, lawyers and business people) are finally catching up to the security professionals, we began to appreciate that cybersecurity is much more than mere legal compliance.

We realized that cyber risk needed to be treated like any other enterprise risk; that is, we should be looking for a program that encompasses administrative, physical, and technical controls designed, documented, enforced (for example, through continuous monitoring and training), and audited across multiple dimensions, such as governance, policy, people, processes, and technology, far beyond requirements prescribed or implied under rules or regulations.

Indeed, cyber provisions today are often quite robust with reps and warranties covering the waterfront of compliance, program depth, vendor management, vulnerability management, training, incident response, and beyond. In some cases, there are even closing conditions or post-closing covenants specific to cyber-related remediation, especially when the borrower has already suffered one or more cybersecurity incidents. It is also no coincidence that cyber reps and warranties have evolved right alongside business models and valuations that are increasingly linked to the collection, storage, and processing of data.

How Could These Cybersecurity Risks be Addressed in the Loan Market?

What can lenders do to minimize their risk? The starting point is sound diligence and drafting of reps and warranties along the lines already discussed. The question is whether a lender's downside exposure is sufficient to warrant more invasive or incisive forms of risk management (such as requiring pre- or post-closing assessments or remediation covenants). We have yet to see such steps taken regularly in the loan market but they are certainly now more often discussed.

How Do Credit Agreements Currently Deal With Cybersecurity? What Could a Basic Credit Agreement Cybersecurity Provision Look Like?

Today, model credit agreements often do not contain cyber-specific terms. However, lenders are increasingly attuned to cyber risk and a wave is forming that we think will end with credit agreements incorporating M&A-style cyber reps and warranties (discussed above). We are now only at the precipice.