How is a reliance on outsourced vendors exposing law firms (and other professional service firms)?

In February 2020, a major vendor to the legal profession suffered a ransomware attack that forced it to take its legal services platform offline for over two weeks. In addition to the inconvenience of having to reschedule matters, law firms were left with the uncertainty of whether confidential client information might have been compromised (whether encrypted by the ransomware, exfiltrated, or both).

The rise of outsourcing

Law firms have historically resisted using third party vendors for the provision of services; firms were reluctant to outsource any function that formed part of what might be termed 'legal services.' Many firms did not outsource at all, preferring to maintain control through on-premises servers and in-house technology staff.

The march of technology has greatly increased the complexity and cost of maintaining in-house systems and, as the sophistication of alternative providers increased, the advantages in cost savings, quality and complexity of services provided, and security capabilities now outweighs the reflex for control and internalization. At least in some cases, clients have encouraged or even pushed firms to take advantage of cost savings that can be obtained through the use of outsourcing. Moreover, the use of technology in court systems and litigation has also made law firms more comfortable with external technological solutions.

Law firms are now outsourcing many critical functions from email to computer security, to document management systems, leading to critical dependencies upon the firms providing services. Many firms focus on the attraction of often substantial cost savings, as well as the fact that major outsource providers generally have and can afford more robust and sophisticated security technology.

Read more about professional service firms' cyber vulnerabilities in 2020 **here**.

From the outside, in: vulnerabilities in outsourcing

When calculating cost savings, law firms should analyze the other side of the balance sheet with the cost of risk associated with depending on a third-party provider. Managing the risks associated with outsourcing critical business processes is a very different proposition from managing internal risk, and the leverage that reduces costs on one side can create pinch points that magnify risk on the other.

What are the implications and impacts of an event at a service provider?

- Inability to serve clients, including delays and the inability to access vital data. This can lead to missing critical dates (affecting business deals, legal filings, litigation, closings etc.). The financial consequences of this can vary from minimal to catastrophic.

- Corruption of data: data sets that have been entrusted to third party providers may be the only version in a specific form, requiring enormous amounts of work to re-create or remediate if the data is inaccessible, or is suspected to have been tampered with or corrupted. Backups may be available (although cyber criminals may attempt to encrypt or delete these backups to ensure that ransoms are paid), but even if available, backups may be dated or may have to be extensively inspected or repaired if there is a suspicion that the data has been tampered with or is not in the format required. Reconstruction of the data set may be possible, but that task may be lengthy (leading to delays and potentially missing critical dates) and costly.
- The impact of the data theft (commonly referred to as exfiltration) will vary according to the type of data stolen:
    - Intellectual property (loss of market/loss of deals/devaluation of the IP)
    - Personally identifiable information or PII (cost of notifications, fines & penalties)
    - Deal information (cancellation or delay of a deal or IPO, compromise of a deal or acquisition/sale/project)
- Unavailability of service (leading to the need to obtain another provider at short notice, with the associated costs and additional work involved in setting up, educating and acclimatizing the new provider)

In this situation, the firm could find itself with a variety of potentially conflicting obligations and associated issues to resolve, including:

- Client contracts requiring notification within a specific time
- Statutory obligations (varying by geography) to report a compromise of PII to authorities
- Statutory obligations to notify parties whose PII has been compromised
- Indemnity obligations to clients
- Indemnity rights under the MSA/contract with the provider
- Duty to notify the incident to insurers (or to notify a circumstance) under policy conditions if it might result in a claim

How will insurance respond?

A firm's **cyber insurance** and **professional liability** coverages become immediately relevant, and the insured should review the situation with their insurance broker to determine the appropriate course of action. The insured should take account of the sensitivity of the matters involved and the potential for litigation against the firm before divulging information to any third party (including an insurance company) and consider engaging qualified external counsel to help navigate issues.

The insurance response will be dictated by the exact circumstances of the event. It will also depend, to an extent, on the contract terms between both the firm and the client and the firm and the provider.

> *"Technology service vendors typically protect themselves in their contracts by way of extreme limitations of liability and hold harmless clauses, but these vary and can contain exceptions. Careful review of these contracts is essential."*
>
> *Tom Ricketts, Senior Vice President and Executive Director, Professional Services Practice, Aon*

Cyber and professional liability insurers' response will not only depend on how far the policies have been tailored to the specific needs of the firm but also, to an extent, on how the liabilities and indemnities are expressed in the client contract and vendor MSA/contract. A firm should review the terms of these agreements with its insurance broker to understand the options that exist and how insurance may apply. It is also critically important to ensure that the insurance policies have been worded to eliminate potential areas of conflict or overlap.

If you would like to discuss any of the issues raised in this article, please contact **Tom Ricketts**.