3 Key Lessons in Vendor Management Highlighted by the MOVEit Cyber Incident

By Casey Waughn, Armstrong Teasdale

If you are anything like me, the company "MOVEit" was not on your radar prior to the end of May 2023. But following the cyberattack experienced by the file transfer company over Memorial Day weekend, it has been hard to go a week, or even a day, without seeing "MOVEit" in a headline.

MOVEit is (or perhaps, was) a popular file transfer system used by many organizations, and particularly by vendors to receive information to process on behalf of companies. Over Memorial Day weekend, a well known ransomware group, CL0P, exploited a vulnerability in the MOVEit transfer software, allowing the ransomware group to gain access to information contained in files that were transferred using MOVEit. After the incident, headlines started to break about the various organizations impacted and the scope of the incident, which by some counts, is estimated to have impacted more than 34 million individuals and 500 organizations.

While there is always an opportunity to consider "lessons learned" following a cybersecurity incident, the MOVEit incident underscores the importance of having sound vendor management practices. In particular, the MOVEit incident highlights three key takeaways: 1) know your vendors (and strive to know your vendors' vendors); 2) solid vendor contracts are crucial for managing risk and clarifying roles in the event of a security incident; and 3) incident response plans or procedures should address vendor vulnerabilities and incidents.

1. Know your Vendors (and Strive to Know your Vendors' Vendors)

MOVEit is a vendor or service provider that offers a tool to organizations to transfer files. But because MOVEit is a file transfer tool, MOVEit was also often used by vendors or data processors who processed data on behalf of or provided services to organizations to receive information from clients or organizations that they provided services to. For example, MOVEit was used by PwC, Ernst & Young (both consultants and accounting firms to organizations), the National Student Clearinghouse (a vendor to colleges and universities), PBI Research Services (PBI) (a vendor to financial institutions), and others. Accordingly, not only was MOVEit itself a vendor to organizations, but MOVEit was often a vendor-of-a-vendor to organizations that were ultimately impacted by the incident.

In the case of the vendor-of-a-vendor posture, many organizations whose data was being transferred to their vendor (via MOVEit) did not know that MOVEit was involved in the transfer or anywhere in the information disclosure chain. However, most state data breach notification laws place obligations to notify individuals and regulators on the owner or licensor of the data, and not on the licensee or vendor of the organization. Because the law is framed in this way, many organizations who were two layers removed from the incident (i.e., MOVEit was used by the organization's vendor) still found themselves announcing the vulnerability, making public notice on their website, and facing the pushback and reputational damage that often follows such

public statements. This also often led to the organization answering questions regarding or defending the use of MOVEit, which it may or may not have been in a position to answer, particularly if it did not know MOVEit was utilized by its vendor to transfer data. Knowing your vendors, and asking your vendors which critical vendors they use to process your data, can help get ahead of some of the questions and necessary information that organizations often need following a vulnerability.

2. Solid Vendor Contracts are Crucial for Managing Risk and Clarifying Roles in the Event of a Security Incident

In the event of a vendor incident, one of the first things most organizations do is look at their contract with the vendor to determine which obligations (and costs) they can impute on the vendor, which roles the parties agreed to take in the event of an incident, and whether their organization now has a right to terminate the contract because of the incident. Most state consumer data privacy laws require contracts between organizations and vendors who process personal data on their behalf to ensure appropriate privacy measures are undertaken, but these laws do not dictate any required terms with respect to security incidents, and state breach notification laws are usually similarly silent on any requirements for vendor contracts.

Too often when examining the agreement following an incident, organizations discover that the indemnity cap in their vendor agreement either expressly excludes security incidents or breaches of confidential information, or only includes damages for third-party claims as a result of the vendor's processing of data, neither of which often cover the costs of remediation and notification that organizations typically incur when an incident occurs.

Even more often, contracts do not specify the roles of the parties or the obligations the vendor has to the organization following an incident. For example, many contracts are silent about the type of information the vendor must provide to the organization about the incident. Since the organization often has limited visibility into the innerworkings of its vendor (including their systems that were compromised), yet the organization has the notice obligations, which often include describing specifically what happened, the information impacted, and how it was accessed, this leaves organizations without the necessary information to achieve their notice obligations, and no way to force the vendor's hand to provide information. Many contracts also do not delegate which party will make notice to individuals or regulators (and pay for such notice), and the organization's right to be involved, or to require the vendor to be involved, in the notice process. Organizations can often push in their contracts to have vendors make notifications to regulators and/or individuals on their behalf in the event that the vendor experiences a vulnerability, and even in doing this, can often retain the right to approve the content of any notice. However, if this contractual language is not present, vendors often throw up their hands and push all notice obligations down to organizations, despite holding the keys to the information necessary to make notice.

Carefully negotiating vendor contracts to ensure there is indemnity and coverage for the organization's costs of remediation and notification, and ensuring that the roles of the parties are clearly outlined so there is no question as to the rights and obligations the vendor and

organization have, can make navigating a vendor incident much smoother, less costly, and can often result in less reputational damage to the organization.

3. Incident Response Plans or Procedures Should Address Vendor Vulnerabilities and Incidents

While many organizations in recent years have developed incident response plans or procedures to be able to spring into action if they directly experience an incident, many organizations' plans and procedures do not contemplate incidents involving their vendors. When an organization receives an email from their vendor that they experienced a security incident and their organization is likely impacted, the organization loses valuable time (and bargaining power) by not acting swiftly following the notification. Failure to act quickly can also increase the risk of missing key deadlines. For example, organizations subject to the General Data Protection Regulation (GDPR) have just 72 hours to make a notification following a suspected personal data breach, and many publicly traded companies will now be subject to the same timeframe with the SEC's new rules aimed at cybersecurity risk management, strategy, governance and incident disclosure.

If an organization does not act swiftly to secure information about the scope and impact of the incident, the organization risks missing these tight timeframes, or not having enough information from the vendor to make meaningful notification. In the event your organization does not have a contract with the vendor that specifies each party's obligations in the event of an incident, or which aspects of the incident response the vendor will pay for, being one of the first in line making demands on the vendor to cover the costs of remediation and notification can also help ensure that there are still funds in the vendor's corner (or, their cyber policy) to cover your organization's efforts to mitigate their incident. Adopting incident response policies and procedures with respect to vendor vulnerabilities can mitigate this risk and ensure that your organization acts swiftly.

While many organizations now operate under the guise that cybersecurity incidents are somewhat inevitable, the above three considerations are proactive and preventive vendor management risk mitigation techniques that organizations can adopt to be more prepared when and if an incident arises.

Casey Waughn *is a lawyer at Armstrong Teasdale who helps clients navigate and comply with complex regulatory regimes, particularly in the data privacy, cybersecurity and white-collar spaces. She assists organizations of all sizes with responding to risk and developing compliance strategies that fit their needs. She is a Certified Information Privacy Professional for the United States (CIPP/US) and frequently speaks on and publishes articles about data privacy topics. She is an active member of the privacy bar and serves as the co-chair of the St. Louis chapter of the International Association of Privacy Professionals (IAPP). Casey can be reached at cwaughn@atllp.com and 314.259.4766.*