2022 CLM Focus Conference
November 2-3, 2022
Washington, D.C.

Assessment and Management of Third-Party Vendor Cybersecurity Risks

I. Overview of Third-Party Vendor Cybersecurity Risks

The frequency and increasing severity of cybersecurity attacks continue to dramatically impact industries worldwide. This panel will provide an overview of the latest cyber threats as they relate to the increasing use of third-party vendors and the growing importance of assessing and managing a company's cybersecurity risks beyond its own systems and processes. It is critical to assess the outer boundaries of your potential cyber vulnerabilities when working with outside vendors, which increasingly have access to all of a company's systems.

Although many companies are implementing cybersecurity plans for their businesses, many fail to address the tangible cybersecurity threats and vulnerabilities associated with third-party vendors. Studies show that security breaches are increasingly caused by a breach in relation to a third-party on a project, or even a third-party's vendor. Companies need to take steps to regulate and streamline processes not only for their own employees, but also in their dealings with third-party vendors.

II. Understanding the Scope of Cybersecurity Risks Posed by Third-Party Vendors.

The world of cybercrime is evolving quickly and businesses must move with it to protect their assets. Third-party vendors are increasingly being relied on to provide critical services to companies, such as email hosting, information technology support, and employee payroll and training. These vendors are typically given complete access to systems of a company, that contain the most important sensitive information of employees, customers, and clients.

It is prudent to formulate a strategy for assessing the risk potential as well as a plan to protect against known areas of vulnerability. The more vendors and third-parties with access to a company's systems, the more important it becomes to conduct a thorough holistic risk

assessment. In addition to vetting third-party vendors, companies should also be cognizant of any potential weaknesses in the security defenses in the supply chain.

III. Cybersecurity Best Practices When Using Third-Party Vendors.

One of the primary methods of protecting against a security breach by a third-party vendor is to conduct proper vetting before the job begins. Proper vetting includes determining what outside parties your vendor employs and assess potential weaknesses, vulnerabilities, or blind spots in the cybersecurity protocols they maintain. Open discussion and planning as well the communication of expectations and proper processes are all vital in minimizing the chances of a security breach.

Businesses should incorporate the practice of requesting system and organizational control reports from each vendor. This includes reports and other information from third-parties and suppliers outlining the cybersecurity measures they employ and how they deal with a breach, etc. Understanding and assessing the cybersecurity controls and plans in place is essential to determining whether they are in line with the standards set for your business. If they do not employ a cybersecurity plan, a business should either require one to be instituted or vet alternate vendors who do have such safety measures in place.

Once a business has assessed the risk factors, it must establish monitoring procedures and controls. Employees and all interested parties should be trained and educated on how to avoid cybersecurity breaches and what to do if one occurs. Create an action plan that is shared with all parties outlining steps to take in minimizing the breach and resolving any issues as quickly as possible. This includes neutralizing the threat, making disclosures required by governmental entities to clients and others affected, determining whether to pay ransoms, consulting with legal counsel and insurers, and handling any public relations fallout.

A critical part of the vendor selection process is the incorporation of strong provisions in any vendor contract regarding their cybersecurity requirements, as well as protocols for addressing data breaches, and shifting the costs and liability in the event of a breach. When there is a data breach, the investigation typically entails identification of the source of the attack, which can often times identify a vulnerability in some system or process. When those vulnerabilities are traced back to a third-party vendor, that vendor should accept responsibility for the breach and provide whatever assistance necessary, financial and otherwise, to address and remedy the breach. If strong contract provisions are contained in a vendor contract which clearly lay out these requirements and responsibilities, the post-breach dispute process can be much more smooth and likely to lead to a favorable outcome.

Businesses should also enhance their insurance coverage, and ensure that their third-party vendors have appropriate insurance, including cyber insurance. Changes in statutes and regulations place increasing requirements on companies, and can explicitly hold a company liable for its third-party vendor conduct. These statutory changes and evolving case law have created an environment ripe for data breach related claims. First-party and third-party cyber insurance coverage should be required for all vendors as they protect companies from claims arising out of a data breach or similar cyber incident, including those brought by clients, customers, or regulatory and administrative bodies. Those claims have increased in prevalence, especially data breach class actions, and have dramatically affected the scope and breadth of coverage.

While the rate for cyber insurance policies has been increasing, there is still a significant share of companies which do not have cyber insurance policies and rely on non-cyber policies to try and cover losses of cyber incidents. The insurance industry has been moving to address this "silent cyber" threat, by specifically excluding cyber claims from non-cyber policies, and the uncertainty of these coverages and potential exposures has prompted the need for further change. A company should not rely on non-cyber coverage of its third-party vendors to provide protection for a data breach of that vendor, and instead should insist on standalone cyber insurance.

IV. The Future of Third-Party Vendor Cybersecurity Management.

Comprehensive data privacy statutes, which typically establish requirements for the handling and processing of personal information, and provide for regulatory, and increasingly private, enforcement of data breaches, are currently top priorities for legislative bodies across the country as well as around the world. These laws have resulted in more exposure to potential cybersecurity claims, including those from and between third-party vendors. Companies employing third-party vendors only increase their potential exposure to liability to statutory obligations and potential third-party claims.

As more states and municipalities enact comprehensive privacy regulations, those provide fertile ground for not only regulatory enforcement actions but potential civil claims and litigation. Cyber claims teams will have to continually monitor legislative developments along with legal counsel to ensure the proper and appropriate handling of claims. It is imperative that the cybersecurity teams of all parties on a project coordinate and plan ahead jointly for any potential breach. Companies are strongly advised to take the additional time needed to thoroughly vet and research the data privacy protocols that their third-party vendors and suppliers employ to protect data.