10/14/2019

The Importance of Data Security for Private Equity and Venture Capital Firms

Cybersecurity is a concern for all industries, but some sectors like private equity and venture capital tend to be targeted more than others due to the nature of their business. The following are some of the top data security considerations for PE/VC firms.

Data security is a top-rated concern for businesses in all industries, and private equity (PE) and venture capital (VC) firms are no exception. The threats to PE and VC firms are so pervasive that in 2015, the Securities and Exchange Commission (SEC) released guidance to help companies manage their security risks.

The Department of Homeland Security has designated October as National Cybersecurity Awareness Month, which makes now the perfect time to review some of the top threats PE/VC firms are up against and the solutions that are at their disposal to help firms manage their information security risks.

The Role PE/VC Firms Play in Cybersecurity Initiatives

All investment firms are at risk of data breaches simply because they operate with sensitive financial information in the digital world. Because PE/VC firms can be an attractive target for cyber criminals, management teams need to be vigilant and thorough in their approach to information security.

First, teams must address the security risks related to their third-party vendors. If software vendors or their placement agents have lax security policies, it puts your firm at risk. PE/VC firms should review their vendors' security policies and get written confirmation that their vendors are committed to secure environments.

Employees are also common areas of unauthorized system entry. Employees should be trained on proper cybersecurity protocols, and checks and balances should be put in place to ensure they are held accountable for their network and online application actions. This is true not only of the PE/VC firm itself, but also of the portfolio companies. PE/VC firms have perhaps a broader risk landscape because of the leadership role they play in their portfolio companies.

One of the ways PE/VC firms can help manage their portfolio company information security risk is by starting with strong policies right out of the gate. Information security and cybersecurity conversations

should take place at the relationship onset when PE/VC firms are evaluating target companies in which to invest.

This is particularly important if PE/VC firms have a significant volume of service providers in their portfolio. The subset of service providers that are *software as a service* (SaaS) providers can be prime targets for unauthorized cybersecurity activity because their core businesses rely on collecting, carrying, and processing client information that is both personal and sensitive. This is just the type of data hackers are hoping to get.

When PE/VC firms invest in SaaS providers, they must encourage those companies to follow proper security protocols so that everybody is well protected. PE/VC firms should add cybersecurity due diligence into their early conversations with SaaS providers. The following precautions can help PE/VC firms manage their SaaS portfolio company risk:

- **Talk to the SaaS company's CIO about the company's information security framework and protocol.** Does the company's information security align with industry-recognized guidelines and frameworks? When was the last time the company performed a baseline risk/gap assessment against a security controls framework?
- **Review the agreements the company has with its third-party vendors.** Does the SaaS company have protections from its third-party risks? Is it part of its vendors' breach notification systems?
- **Get written confirmation that the company's encryption and firewall are up-to-date.** Documentation of an organization's cybersecurity protection is vital, and will provide your PE/VC firm an idea of the protections already in place and whether they are sufficient for the activities the company conducts and the data with which it works.
- **Review the company's employee training programs for cybersecurity and other information security initiatives.** Because SaaS providers are key targets for cyber attacks, it's vital that the company train its employees on the role they play in protecting the company's sensitive information. Training programs also speak to how seriously the company takes its information security risks and whether the culture of cybersecurity is pervasive in the organization.
- **Assess policies and procedures surrounding data privacy practices.** Does the company include policies on "bring your own devices"? Does it have a plan for what happens if a device that can access the network is lost? Policies and procedures around the small things are just as vital as the protections for the network.
- **Explore purchasing insurance policies to cover data breach losses.** PE/VC firms that have a significant number of SaaS providers in their portfolio may want to consider a cyber liability policy for either their firm or for their portfolio companies.

An additional step that PE/VC firms may choose to take is to encourage their target company to issue a System and Organization Controls (SOC) 2 report.

What Are SOC 2 Reports?

A SOC 2 report is an inspection of a service organization's non-financial controls from a CPA firm. The security, availability, processing integrity, confidentiality, and privacy of important data are not addressed in a traditional financial statement audit, so PE/VC firms will benefit from requiring a potential new target to commission one.

A clean SOC 2 report assures interested clients and potential investors that the service provider protects the sensitive and private information of its employees, vendors, and customers. There are two types of SOC 2 reports. SOC 2 Type 1 reports cover management's description of a service provider's system and suitability and design of controls at a point in time. SOC 2 Type 2 reports cover management's description of the system and *operating effectiveness* of its controls over a selected period of time.

Either type of SOC 2 report will be valuable to a PE or VC firm looking to invest in a SaaS portfolio company because of how costly data breaches can be for service organizations. If a SaaS company's systems are breached, it could lose clients, future sales, and standing in the industry. A deteriorating reputation can produce unpredictable losses to both the SaaS provider and its investors.

Where to Find Help

The SEC data security guidance provides a good starting point for PE/VC firms that want to improve their cybersecurity approach. It encourages PE/VC owners to conduct regular technology assessments, implement policies and procedures, and create strategies that will prevent, detect, and respond to cyber threats.

It is also helpful to bring in a qualified professional. A trustworthy CPA can consult on data security issues or can begin the audit proceedings for a SOC 2 examination.

For more information about what PE/VC firms can do to address data security concerns, please contact us or check out our upcoming webinar.