ASSESSING A REGISTERED AGENT’S SECURITY MEASURES

Today, the importance of cybersecurity goes without saying. It’s difficult to make a business’s proprietary information and systems available to employees, while still protecting the information from unauthorized access. This task becomes more complex when third parties have access to non-public company information and systems. An organization needs to act not only to protect itself but to provide guidance to clients to help them protect their information.

When considering third-parties with access to sensitive data, one seldom considers the vulnerability created by a company’s choice of registered agent. A registered agent is a conduit for important government documents and service of process (SOP) to the corporation, LLC or other statutory entity. To perform this function, the registered agent needs information about the company, including individuals authorized to accept SOP. As a result, a breach of a registered agent service provider’s database can expose “personally identifiable information” (PII) and other sensitive information.

INCREASING REGULATORY OBLIGATIONS FOR DATA SECURITY

As businesses contend with well-publicized security breaches, an increasing number of jurisdictions have enacted laws to cover data protection.

In the United States, all states—plus the District of Columbia, Puerto Rico, and the U.S. Virgin Islands—have their own database security breach laws. State laws and regulations generally specify the definition of a breach and the requirements for providing notice of a breach to affected parties. In the case of a breach of a third-party registered agent’s network, a business looks to state statute to determine the registered agent’s obligations to the business.

New York’s cybersecurity regulations (NYCRR 500 Part 23)—which went into effect on March 1, 2017—provide an example of one state’s approach to cybersecurity. These regulations address the cybersecurity of financial institutions and outline specific security measures for any third-party service provider that maintains, processes or otherwise electronically accesses non-public information through its relationship with a financial institution. Businesses subject to the regulations must have written policies and processes regarding third parties. A business must perform due diligence in evaluating third parties’ cybersecurity capabilities and ensuring minimum security measures are in place. The business must also perform periodic assessments of the third party’s security procedures.

California’s Consumer Privacy Act of 2018—which goes into effect January 1, 2020—imposes a broad range of requirements for businesses that collect or sell personal information. These

continued on page 2
include disclosing to consumers the purpose behind the information being collected, granting consumers the right to delete that information, and other obligations.

J urisdictions around the world have also addressed cybersecurity. In the European Union (EU), the General Data Protection Regulation (GDPR) — which went into effect on May 25, 2018 — requires that a business work only with data processors (vendor partners) that guarantee compliance with the regulation. The United Kingdom (UK) and Switzerland have data protection requirements in line with those found in GDPR. Australia also has mandatory data breach reporting.

WHY HANDLING EVERYTHING IN-HOUSE MAY NOT BE THE SOLUTION

It is tempting for a business to think it can maintain system security by having an in-house registered agent, rather than face the risk of using a third-party registered agent.

However, a business (particularly one with limited resources) that keeps its information processing and security controls internal may actually be compromising its security and efficiency. Moreover, it could wind up costing more to retain information processing and security controls in-house than by contracting with a third party.

See “The Risks of Using an Individual as Your Registered Agent” for more information on the issues created when an individual serves as a Registered Agent.

SELECTING YOUR REGISTERED AGENT

Business efficiency and price are not the only factors to consider when selecting a Registered Agent provider. A detailed inquiry into the company’s security procedures is essential.

According to Third-Party Cyber Risk & Corporate Responsibility, steps to consider include the following:

- Verify that a third-party registered agent is knowledgeable and trustworthy regarding security measures.
- Ensure those at the company who work with the third-party registered agent ask the right questions, and follow-up on the answers received before providing access to internal data or systems.
- Establish meaningful audit procedures and consequences for violating audit requirements that are written into contracts with vendors from the negotiation stage (this includes procedures for handling data breaches—prompt notification, as well as cooperation in investigating and remediating the breach).
- Ensure that the people within the business who can identify and address security concerns are involved in the negotiation process.
- Cut off the registered agent’s access to the company’s internal data when the relationship is terminated.

Effectively securing sensitive information has never been more important or challenging for organizations. Learn how to effectively secure data with the ACC Model.

SERVICE OF PROCESS CONSIDERATIONS

A registered agent must be available for service of process on a business. Thus, it’s imperative that the business considers non-digital security issues, as well as digital. Specifically, when comparing registered agent options, a business should keep in mind the following service and security considerations:

- Service of process intake: Is the registered agent always available and physically present at the registered office during normal business hours? Is there a multi-point service-of-process intake verification process?
- Service of process verification: Does the registered agent verify all hand-delivered service of process?
Building security: Is the registered agent’s intake location a business office with security? Or does the intake location lack effective security (low-security business office or even a residential address)?

Notification: Will the company receive instant notification of service of process received, including a summary with requisite and relevant information (plaintiff, defendant, answer date, nature of action, etc.)?

Universal security protocols: Are security safeguards in place at all locations of the registered agent (not just the headquarters or main office locations)?

Tools and tracking of compliance tasks: Does the registered agent provide a compliance calendar, reminders for statutory annual report filings and e-filing capability?

In addition to considering whether a third-party registered agent provides the best service at the lowest price, it’s also important to evaluate the registered agent’s commitment to service, technology and security best practices in order to mitigate risk.

CONCLUSION

The issues and logistics of allowing a third-party registered agent access to a business’s data are complex. Having a comprehensive security strategy for a third-party vendor is a critical component of a company’s risk management program.

LEARN MORE

To learn more about how CT can help you manage your compliance requirements, contact your CT representative or call 855.316.8948 (toll-free U.S.).