Compliance & Ethics Professional®

August 2016

A PUBLICATION OF THE SOCIETY OF CORPORATE COMPLIANCE AND ETHICS

www.corporatecompliance.org

Meet Joel A. Rogers

CEO of Compliance Wave
Red Bank, New Jersey

See page **16**

by Jane Zsigmond, CCEP, CCEP-I

Who's covering third (parties)? Controlling access to data on SaaS software

» Ensure third-party vendor contracts contemplate controlling the vendor's employee access to company data.

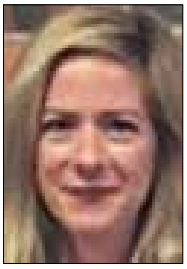
» Ask third-party vendors about their existing compliance programs and IT security protocols to ensure the vendor's employee access to your company's data is limited and is frequently monitored by the vendor.

» Monitor and control third-party vendors' access to data through an annual vendor certification program.

» Assign responsibility to a business leader and follow up to ensure that he/she complies with the company's protocols to control third-party vendor access to data.

» Track the use of SaaS programs to increase transparency and ensure the responsibility of the business leader is transferred appropriately when the company experiences employee turnover.

With IT departments and senior leadership encouraging software as a service (SaaS) software applications for the management of company business, it can be easy to overlook the issue of managing and limiting users' access to these programs when the primary focus is on the anytime/anywhere access and the benefits for IT resources.



Zsigmond

Although some companies have implemented Identity Access Management (IAM) tools for managing employee access to software applications, these IAM tools are designed to give companies control over managing and limiting employee access to their software programs, but they are not designed to control a contractor, consultant, or other third-party vendor's access. Even for those companies with IAM tools, the issue of unauthorized vendor access may remain an unresolved and unmonitored potential for exposure, so compliance officers need to start asking, "Who's covering third parties?"

> Typically, the relationship between a company and its vendors is managed by the relevant business or department leader.

Allowing access

Typically, the relationship between a company and its vendors is managed by the relevant business or department leader. The business leader primarily interacts with the vendor's account representative, and together they are responsible for ensuring that products or services are delivered in a satisfactory manner within budget. For the company, the interaction with the vendor's

employees is minimal, as is the nature of vendor agreements. For a company to have regular interaction with the vendor's employees would defeat one of the benefits of the third-party/vendor arrangement.

Oftentimes during the course of a company's relationship with a vendor, the company may find it necessary or essential to allow the vendor access to company information through company software programs in order for the vendor to fulfill its responsibilities. For licensed software, that requires the download and installation of software to an employer-issued computer, and the computer (and the software installed on it) is ordinarily surrendered by the vendor's employee at the end of his/her employment. However, with the increasing popularity of SaaS software applications, controlling the access of a vendor's employees to a company's SaaS software applications is at risk of being overlooked by the company when it comes to managing third-party vendors and data security.

In the common scenario above, the company's business leader rarely interacts directly with the vendor's employees, so when the vendor experiences employee turnover, the company is more-or-less unaware or impacted by these changes. Moreover, when the vendor experiences employee turnover, it seems reasonable to expect that the vendor would deactivate their former employee's access to clients' SaaS applications in a timely manner, but is that really what's happening in practice? In some cases, the answer is "yes," but in many cases, the answer is "no" or "usually."

Without an IAM-type tool to manage vendor access to company data, compliance officers should consider adopting standard operating procedures for managing and controlling third-party access to company data.

The compliance plan

The first step in controlling unauthorized access to company data by a vendor is to take an inventory of the existing SaaS software applications used by the company's departments or divisions. Once the compliance officer has taken stock of the company's SaaS software applications, he/she should identify those company departments or divisions that utilize these SaaS applications and determine which of these applications are accessed by contractors, consultants, and other third-party vendors.

The first step in controlling unauthorized access to company data by a vendor is to take an inventory of the existing SaaS software applications used by the company's departments or divisions.

Next, the compliance officer should identify which of the company's business leaders manages these vendor relationships and require that the business leaders request from each vendor a list of the vendor's current employees who have access to company data via SaaS software applications.

Ideally, the vendor contract contemplates access to the company's proprietary information and includes language

requiring the vendor to adopt IT security practices that uphold the vendor's confidentiality obligations and ensure the vendor regularly reviews its employee access to clients' software applications, so that only those vendor employees with a "need to know" have access to these programs. The compliance officer should review existing vendor contracts for this language and consider whether a contract addendum is necessary or required to include vendor obligations regarding IT security practices and protocols for limiting access for vendor employees. It is also important for the compliance officer to educate his/her Legal department on the issue and ensure the attorneys understand the importance of including contractual clauses that require the vendor to implement standard operating procedures concerning data security and access, particularly in cases were the vendor's access to company data is via SaaS software applications. For SaaS applications holding highly sensitive company data, such as financial information or personally identifiable information (PII), diligent compliance officers may consider adopting an annual vendor certification program whereby the company requires its vendors with access to SaaS applications to certify that they have reviewed their user access rights and certify that their employees' access is current and necessary in order for the vendor to satisfy its obligations to the company.

Conclusion

As SaaS continues to become the standard platform for software applications, there will be new programs that emerge to assist companies with managing SaaS access. However, until those solutions are available, adopting a process, such as these simple steps, will help compliance officers manage and control vendor access to company data. ✳

Jane Zsigmond *(zsigmond.jane@gmail.com) is Chief Privacy Officer and Director, Compliance in Denver, CO.*

Thank You!

Has someone done something great for you, for the Compliance & Ethics profession, or for SCCE?

If you would like to give recognition by submitting a public "Thank You" to be printed in *Compliance & Ethics Professional*, please send it to liz.hergert@corporatecompliance.org. Entries should be 50 words or fewer.