**Distrust of Vendors Raises Security, Compliance Questions**

Apr 26, 2016

Many companies don’t trust the vendors they share confidential data with, according to a recent Ponemon Institute survey.

The survey of 600 individuals across industries found that more than a third of U.S. businesses (37%) believe that their primary third-party vendors wouldn’t notify them in the event of a security breach involving “sensitive and confidential information.” In addition, 73% of respondents said that fourth-party to "Nth”-party [an unknown number in a series of numbers] vendors – subcontractors or indirect service providers employed by a third-party vendor – would “fail to notify” if a breach occurred.

The survey, “[Data Risk in the Third Party Ecosystem](http://www.buckleysandler.com/uploads/1082/doc/Data_Risk_in_the_Third_Party_Ecosystem_BuckleySandler_LLP_and_Treliant_R....pdf),” was commissioned by law firm BuckleySandler and Treliant Risk Advisors to reveal the challenges facing firms trying to protect client information when sharing data with third parties, according to *Legaltech News.* Companies surveyed have a vendor data risk management program and were asked to only consider their outsourcing relationships in which they share “sensitive or confidential information or involve processes” that require vendor access to that data.

The survey revealed difficulties with “mitigating, detecting and minimizing” risks posed by third parties handling company data. According to the survey, companies lack faith in outside data handling and are not able to properly manage it. The findings show:

* About half (49%) of companies said they experienced a breach caused by vendors, while 16% said they weren’t sure if a vendor was to blame.
* 73% of companies said they see vendor-related cybersecurity incidents increasing.
* Most companies find it difficult to manage vendor-related cyber incidents, with 65% saying they “don’t have the internal resources to check or verify” when evaluating vendors’ security and privacy practices.
* 58% of companies said they cannot determine whether vendor “safeguards and security policies are sufficient to prevent a data breach,” leaving 41% who said they are sufficient.

“The reliance solely upon contractual agreements instead of audits and assessments to evaluate the security and privacy practices creates significant risk,” Margo H.K. Tank, partner with BuckleySandler, told *Legaltech News*. “Companies will need to establish and track metrics regarding the effectiveness of the vendor risk management program and establish vendor risk management committees.”

According to the survey, for many companies, information governance in vendor relations should be strengthened. For example, only 31% view their vendor risk management program as “highly effective,” while 38% said they don’t track metrics on their programs’ effectiveness. In addition, the majority (62%) admitted that “their boards of directors do not require assurances that vendor risk is being assessed, managed, or monitored appropriately, or they are unsure.”

“Companies must understand managing data risk is not merely a compliance and contract issue but a fundamental strategic challenge in which personal data, intellectual property and transactional records must be protected from third, fourth and nth-party risk,” Tank said.

ARMA International has a number of resources to assist organizations in contracting with third parties for records and information management services, as follows.

**Free *Information Management* magazine articles:**

* **“**[From RFP to Selection: Guidance for Outsourcing RIM Functions](http://imm.arma.org/publication/?i=241225&p=24)**”**
* “[Seven Things Records Destruction Vendors Are Afraid to Tell You](http://imm.arma.org/publication/?i=291982&p=42)”

**Web Seminar:**

* [Managing the Privacy and Security Risks of Vendor Relationships](http://www.arma.org/go/evt/CFWS4430)

**ARMA International standards workgroup guidelines and technical report:**

* [*Contracted Destruction for Records and Information Media*](http://www.arma.org/go/prod/a4919)
* [*Guideline for Evaluating Offsite Records Storage Facilities*](http://www.arma.org/go/prod/a4734)
* [*Guideline for Outsourcing Records Storage to the Cloud*](http://www.arma.org/go/prod/a4924)
* [*Understanding Electronic Records Storage Technologies* (ARMA TR 26-2014)](http://www.arma.org/go/prod/a4958)

**Source:**  
[LegalTechNews.com](http://www.legaltechnews.com/id=1202754163270/Distrust-of-Vendors-Raises-Questions-on-Data-Security-Regulatory-Compliance?slreturn=20160315001013)