Data Risk in the Third-Party Ecosystem

Ponemon INSTITUTE

Research sponsored by BuckleySandler LLP & Treliant Risk Advisors LLC
Independently conducted by Ponemon Institute LLC

Buckley Sandler LLP

When it comes to data security, US companies have serious concerns about their third-party vendors—and with good reason.

The Problem

Data breaches are on the rise and the percentage of those data breaches caused by third-party relationships is also expected to rise. In our recent survey, "Data Risk in the Third-Party Ecosystem," conducted by the Ponemon Institute, 49% of respondents indicated their company had experienced a data breach caused by a vendor, and 73% expected the number of third-party-related cyber incidents to increase. In fact, many of the largest and most publicized breaches that have occurred since 2015 can be traced to third-party relationships.

49% of respondents indicated their company had experienced a data breach caused by a vendor, and 73% expected the number of third-party-related cyber-incidents to increase.

As companies continue to embrace dynamic outsourcing and infrastructures, the inherent risks to data become much more difficult to manage. It is no longer possible to think of an enterprise as a single organization supported by a well-established and controlled "chain" but rather as the entry point to an ecosystem of suppliers, vendors and service providers each with their own sub-set of providers. These third-, fourth-, and nth- party relationships, and the risks associated with them, must be considered and managed when dealing with third-party risk. (Third-party vendors are direct service providers hired by a company. Fourth- through nth-party vendors are indirect service providers or subcontractors hired by a third-party vendor.)

Regulatory Concerns

Regulators are keenly aware of the risk posed by third parties to data assets and continue to publish guidance and update requirements with respect to managing it. Regulatory guidance generally requires companies do the following with respect to third parties:

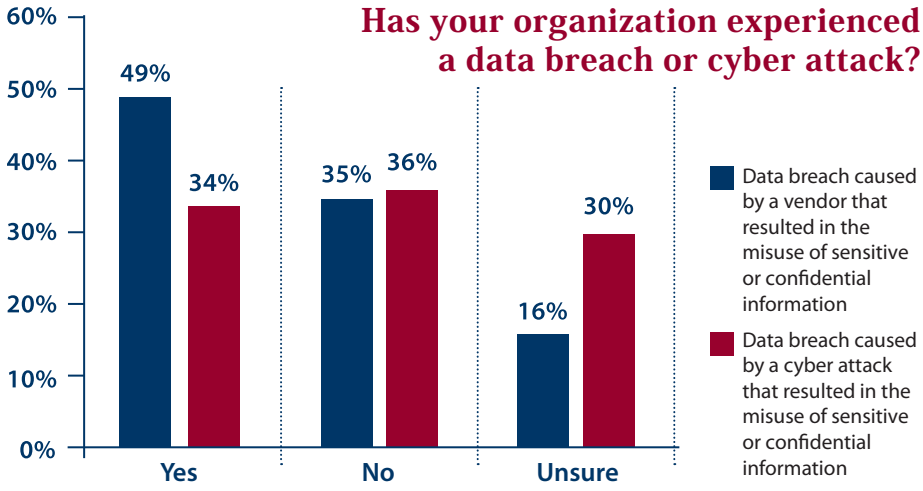
- Perform risk due diligence/assessment prior to establishing a relationship with a vendor
- Incorporate security standards and expectations into vendor contracts
- Limit data sharing and access to only those necessary for business purposes
- Perform initial and ongoing assessment of third-party vendors
- Require third parties to report any event or change that impacts the security of company assets

For those companies that do not adequately identify and manage third-party data risk, the impact of outsourcing fourth- and nth- party relationships will become all too apparent in their post-breach investigations.

73%

Respondents felt an nth- party vendor would fail to inform them of a data breach.

Has your organization experienced a data breach or cyber attack?



The Risks

Many of the survey respondents noted the challenges of implementing effective third-party risk management programs. Taken together, the answers provide insight into some of the common failings plaguing third-party management programs:

- **One size fits all** – assumes all vendors represent equal risk
- **Risk criteria** – not customized to company risk environment and not updated over time
- **Contractual language** – assumes standard vendor contract language is sufficient to manage third-party risk
- **Self-assessments and third-party audits** – considered guarantees of adequate compliance
- **Third-party risk** – not a priority for board and senior management
- **Beyond compliance** – focus is on risk being a compliance function but it is a fundamental business survival issue

The Survey Results

The Ponemon Institute surveyed 598 individuals across multiple industries who are familiar with their organization's approach to managing data risks created through outsourcing.

60% say they do not have an inventory of third-party vendors, and 63% say there is no centralized control over third-party relationships.

62% say their boards do not require assurances on vendor risk assessment, 45% say it is not a priority, and 39% indicate the information is provided only after a security incident.

Only 38% say the organization tracks metrics regarding the effectiveness of the vendor risk management program.

69% believe that over 20% of their vendors are outsourcing their company's sensitive and confidential data to n^{th} parties.

71% indicate their company has no visibility into the n^{th} parties that access sensitive and confidential information.

Only 35% say their company is effective in detecting third-party risk and even fewer (22%) say they are effective in mitigating third-party risk. The percentages are much lower for fourth- and n^{th}-party risk.

61% rely on contractual agreements to gain visibility into vendors' practices, and 55% rely upon their third-party vendor to notify them when their data is shared with n^{th} parties.

Only 35% say that a frequent review of vendor management policies is conducted to ensure the ever-changing landscape of third-party risk is addressed.

What is Needed

Common elements of an effective third-party risk management program:

- **Risk identification** – relevant risks, evaluation criteria, and levels defined
- **Governance** – risk management extends from board to management to operations
- **Responsibility and accountability** – defined roles, responsibilities, and authority
- **Organization and resourcing** – appropriate for company attributes and risk environment
- **Third parties** – identified, inventoried, and risk ranked
- **Contracts and agreements** – incorporate security and data risk requirements
- **Third-party assessment and enforcement** – appropriate for risk level and performed consistently
- **Training and awareness** – tailored for board, senior management, and employees
- **Change management** – program adjusted in response to internal and external change
- **Reporting** – metrics and reporting to management and board on risk and program effectiveness

How BuckleySandler Can Help

Effective third-party management programs address the basic requirements necessary to effectively manage and mitigate risk. Survey respondents indicated they struggle due to a lack of resources, ineffective governance structures, incomplete vendor inventories, one-size-fits-all processes, and little or no change management capability. At BuckleySandler, we bring our deep regulatory expertise and industry experience to providing our clients with services to meet those challenges. In addition to identifying legal requirements that may apply specifically to your company, we also can help with the challenges identified in the survey:

Third-party risk management

- Legal and regulatory requirements
- Board awareness and management training
- Program design and governance structure
- Policies and procedures
- Risk identification and evaluation framework
- Vendor program – assessment & gap analysis

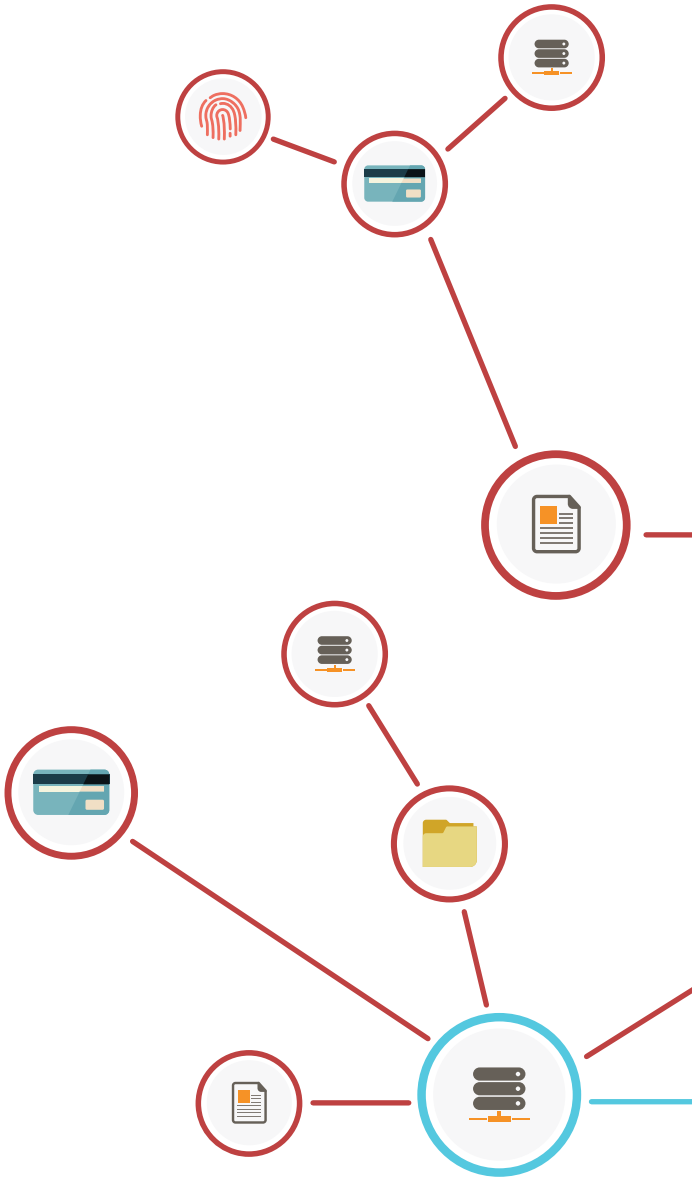
Contract management

- Third-party contract support
- Contract language

Vendor assessment / response to queries

- Due diligence
- Compliance assessment
- On-site reviews
- Responses to vendor/regulatory inquiries

Buckley Sandler LLP



BuckleySandler LLP provides premier legal counsel to protect and support the nation's leading financial services institutions, corporations, and individual clients. With more than 150 lawyers in Washington, DC, Los Angeles, New York, Chicago and London, we offer a full range of litigation, transactional, compliance, and regulatory services.

Our Privacy, Cyber Risk & Data Security practice assists clients in proactively developing, implementing, and evaluating data risk mitigation strategies, enterprise security and privacy programs, cybersecurity and breach response capabilities, control environments, and reporting processes.

Margo Tank
Partner, BuckleySandler, LLP
202.349.8050
mtank@buckleysandler.com

Douglas F. Gansler
Partner, BuckleySandler, LLP
202.349.8058
dgansler@buckleysandler.com

Elizabeth E. McGinn
Partner, BuckleySandler, LLP
202.349.7968
emcginn@buckleysandler.com

James T. Shreve
Counsel, BuckleySandler, LLP
202.461.2994
jshreve@buckleysandler.com