HOW DO YOU QUANTIFY 3RD PARTY RISK?

Half of a company's cyber-risk is from 3rd parties

CASE STUDY

Analyzing & Reducing 3rd Party Risk Using a Statistical Approach

- **Brought Predictability** to the randomness of data breach
- **Accurate Assessment** met regulators request for an accurate methodology
- **Reduced Risk** 3rd party by 50%, company by 25%, focusing on 2 vendors
- **Saved Money** via vendor triage & no questionnaires
- **Enabled Senior Management** weighed business priorities against cyber-risk

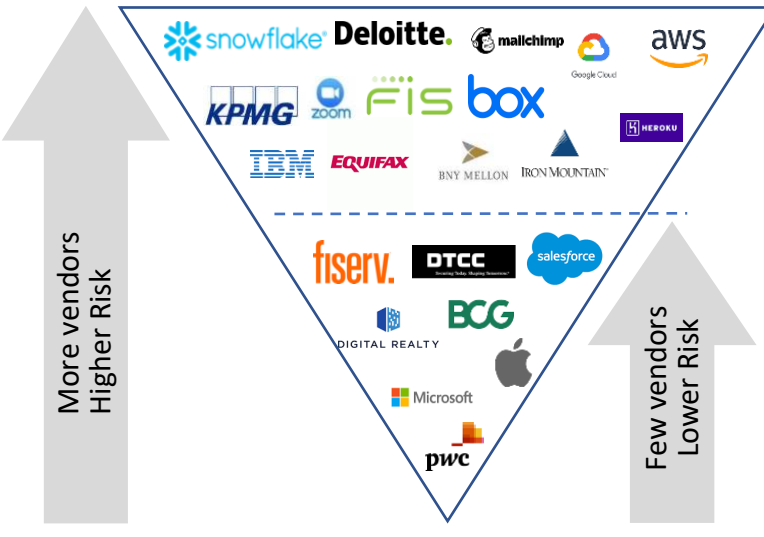
About 3rd Party Risk

Your risk is dependent on the number of 3rd parties: the more vendors with access to your data, the more likely one will cause a data breach. This aggregate risk can be calculated simply by adding probabilities from each of your vendors, from a statistical model. An accurate model will also often find large differences between vendors and typically a few vendors will represent a large proportion of your aggregate risk. Focusing your mitigation efforts on these vendors will substantially and quantifiably reduce your 3rd party risk, and your company's cyber-risk overall. Your aggregate risk cannot be calculated using questionnaires or maturity scores, but we can help you measure your aggregate risk with an accurate and testable, statistical model.

About the Model

VivoSecurity assesses the risk of a data breach from 3rd parties, using a SR11-7 compliant patent-pending empirical regression model that is based upon overall employees count, and ratio of employees with certain certifications in cybersecurity, compliance and IT.

These measures have been found to be strongly predictive and statistically independent for forecasting a reportable PII data breach caused by: 1) malicious outsider, 2) malicious insider, 3) an accident and 4) a lost or stollen device.



VivoSecurity

1 A complete vendor list provided many advantages

Eliminating questionnaires saved time & money

Our client turned over a complete list of 50 vendors (the complete list is not shown), including 32 vendors that could expose PII. No further information was needed and all data needed for the statistical model was supplied by Vivo.

Regulators saw a comprehensive process

A complete list, including even vendors that cannot expose data, allowed Vivo to create a report that documented the comprehensive nature of the analysis for regulators.

Accuracy was assessed by a testable prediction

Including vendors that could not expose data also allowed our client and regulators to better assess the accuracy of the model, by comparing a future forecast from the model, with a history of data breaches. A larger pool of vendors produces a more accurate assessment (please contact Vivo for more information about testing model accuracy and for a model document).

The model forecast 1.3 data breaches per year across all vendors, and we found an average of 1.1 data breaches per year over the last 20 years. Management considered this future forecast to be very close to the history of data breaches since the model is foreword looking and does not reflect past data breach rates or security postures. Also, data breaches are increasing year-by-year.

Vendor	PII
DNAnexus	3,000,000
SumoLogic	3,000,000
SoftFile	3,000,000
Snowflake	3,000,000
CyberLink (Rose ASP)	3,000,000
Synergen Health	3,000,000
Iron Mountain	3,000,000
Amazon Web Services (AWS)	3,000,000
Skedulo	100,000
Carbonite	100,000
Asuragen	100,000
eFax (J2 Global)	100,000
LabVantage Solutions, Inc.	100,000
Worldwide Clinical Trials	100,000
Google Applicaitons	100,000
Baylor Genetics	10,000
Histo-Tec Laboratory	10,000
PanAmericom	10,000
ClinCapture EDC	10,000
Ashion Analytics	10,000
Florence Healthcare, Inc.	10,000
Medable, Inc.	10,000
Prevention Genetics	10,000
Box	10,000
GRM Document Management	10,000
MERA Switzerland AG	10,000
Mt Sinai (Sema4)	10,000
Atlassian	10,000
SalesForce	10,000
Success Factors	2,000
Stem Express	1,000
Zoom	1,000
Virtru	0
Brivo	0
Document Center, Inc.	0

2 Breach probabilities brought predictability

Vivo's statistical model forecasts PII data breach based upon the number of employees with certain certifications. We found empirically, that these certifications are highly predictive and statistically independent. These certifications also bring insights about a vendors cybersecurity spending and compliance culture.

For each vendor, Vivo collected this headcount information **without the assistance of the vendors**, then calculated probabilities for each vendor across 8 different data breach sizes, and finally summed probabilities to forecast the aggregate probability—the probability that some vendor would cause a data breach.

Predictability was brought to the randomness of data breach

With aggregate probabilities, our client's senior management could understand the frequency of data breach across a range of data breach sizes and decide the companies risk appetite (see table right).

Management weighed business priorities against cyber-risk

Breach Size (People Affected)	Aggregate Breach Frequency (annual probability)	
	Company	Industry Median (σ)
1000	5-years (20%)	29-years (45) (3%)
10,000	10-years (10%)	63-years (85) (1.5%)
100,000	4-years (25%)	13-years (10) (8%)
1,000,000	11-years (9%)	43-years (42) (2%)
10,000,000	89-years (1.1%)	374-years (324) (0.3%)
100,000,000	474-years (0.2%)	2356-years (2273) (0.04%)

The table shows the mean years between data breaches across all critical vendors, for six of the eight data breach sizes. For example, a data breach affecting 10,000 people can be expected every 10-years on average across any one of the 32 critical vendors.

Vivo also provided a cross industry median, for comparison. For example, the cross industry median for the same sized data breach is once in 63-years, on average.

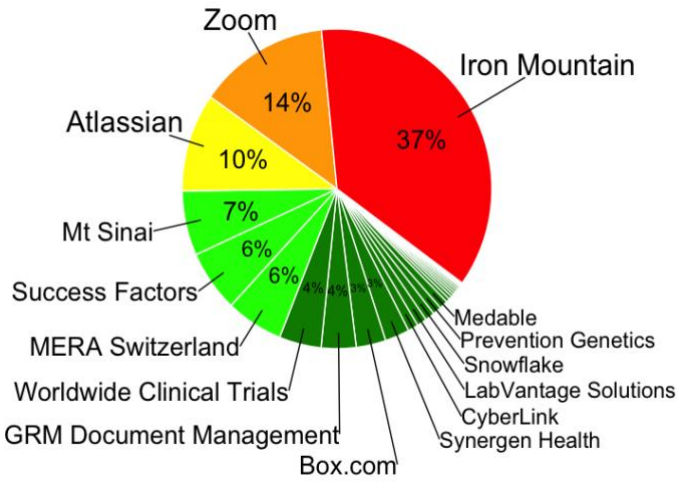
3 Reduced risk by focusing on just two vendors

An accurate model will find large differences between vendors for the probability of a data breach, and typically, just a few vendors will account for most of the 3rd party risk.

Vivo calculated each vendors contribution to aggregate risk for each of the eight data breach sizes, to reveal the vendors that contribute most. The pie chart shows each vendor's contribution for a data breach affecting 10,000 people.

Two vendors, **Iron Mountain** (accounting for 37% of aggregate risk) and **Zoom** (accounting for 14% of aggregate risk) together account for **51%** of aggregate 3rd party risk. A data breach could occur by any vendor, but there is a 51% chance the breach would occur by Zoom or Iron Mountain.

Vivo calculated that mitigating the risk from **Zoom** and **Iron Mountain** would reduce 3rd party risk by half, taking the probability for this breach size from once in 10-years to once in 20-years, on average. This is still significantly worse than the cross-industry median, but acceptable to senior management for now.



Reduced 3rd party risk by 50%; company risk by 25%

4 Simple mitigation plans saved money

Focusing on just two vendors saved money

The table shows our clients mitigation plan for **Iron Mountain** and **Zoom**. Since our client was not encrypting backup media sent to **Iron Mountain**, the risk could be mitigated by simply encrypting backup media.

Zoom was also an easy risk to mitigate. Our client was presenting patient data during recorded **Zoom** meetings and saving them within **Zoom**. This risk could be mitigated simply by training employees not to save meeting recordings in **Zoom**, and instead save recordings locally.

Vendor	Risk Source	Mitigation
Iron Mountain	Unencrypted backup media	Encrypt backups
Zoom	Recording meetings with patient data	Don't save recordings in Zoom

Regulators saw a mature process

Our client was able to show regulators 1) a comprehensive process for 3rd party risk, 2) the accuracy of the model, and 3) justify a mitigation plan that focused on just two vendors.

About Us

We are enabling companies to improve cybersecurity and reduce costs, by bringing predictability to the randomness of data breach, using data analytics and A.I. We are scientist and statisticians, bringing our customers the most advance tools and datasets in regression modeling, AI and machine learning.

Let us help you view your 3rd party risk from a new perspective. We will help you • reduce risk • save money • satisfy regulators • impress new customers and • bring predictability to the randomness of data breach.

Dr. Thomas Lee, CEO and cofounder,
BS Physics & EE, University of Washington, PhD Biophysics, University of Chicago.

Dr. Spencer Graves, leads our modeling and data analysis,
PhD Mathematical Statistics, University of Wisconsin.

VivoSecurity
inquires@vivosecurity.com
telephone: (650) 919-3050