Assessing the Effectiveness of Third-Party Risk Management using Quantitative Models

A new protocol for **Internal Audit** to assure that third-party data breach risk is within management's risk-tolerance.

Authors:

Axel Troike
EU, Executive Consultant & External Auditor with focus on Business Architecture & Data Governance

Thomas Lee, PhD
Silicon Valley, VivoSecurity
ThomasL@VivoSecurity.com

David Hann
UK, DHann Consulting, Internal Auditor & TPRM at Lloyds Banking Group, KPMG, PwC, Deloitte, IHS Markit

Contributors:
Peter Davis: CISA, CISSP, CISM, CGEIT, governance, audit and security consultant; Neal Scott: Risk & Compliance, Internal Audit; John Lazar: CISA, Internal Audit; Osasere Peter Owegie: CISA, CICA, CNSP, ITIL, Head Internal Audit, authority on 27001; Shawn Wilde: CIO, authority on Healthcare, HIPAA & TPRM; Tom Kuang: CCNA, CISSP, CISO; Teresa Joyce: CISA, CISSP, CISM, CISO.

Abstract

Have you ever wondered what motivates an **Internal Auditor**? Is it improving a process important for the business through determined investigation? Is it creating a proposal that is first welcomed by the business, approved by the Board, implemented by the organization, and finally recognized by the company as having provided quantifiable benefits?

Third-party risk management (**TPRM**) can be such a process. Third-parties are an important enabler for the business. However, they also bring risk from data breach. Third-party data breach risk is significant and increases with the number of vendors that can expose a company's data. But most TPRM programs do not measure or directly manage this **cumulative-risk** despite most regulations and many frameworks requiring it. Ineffective management of cumulative-risk can limit a company's ability to leverage third-parties. Ineffective management of cumulative-risk can also undermine the goals of internal cybersecurity investments and leave a company over-exposed.

We show how **Internal Audit** can use **new statistical models** to work with the TPRM team to objectively test that third-party data breach risk is within management's risk tolerance. We also explain changes **Internal Audit** can recommend, that allows the TPRM team to manage cumulative-risk if it exceeds management's risk tolerance or if it is limiting the ability of the business to leverage third-parties.

Scan for an electronic version of the full white paper.

Report

Value and Risks from Third-Parties

Third-parties bring efficiency and new technologies, and are an important part of most companies' business, products, and services. Just considering cloud services, we now have Infrastructure as a Service (IaaS) with companies like AWS; Platform as a Service (PaaS) with companies like Heroku, Microsoft, Google and IBM, and Software as a Service (SaaS) with companies providing hosted email like Microsoft and Google, risk management software, HR services, and customer relationship management like Hubspot and Salesforce. We have third-party services for monitoring fraud, third-party services providing transaction processing such as online banking, third-party services for marketing and lead generation, outsourced call-centers, and third-parties providing accounting services. Third-parties can also provide low-code/no-code platforms such as Salesforce and ServiceNow.

Third-Party Risk Management (**TPRM**) is tasked with managing the risks associated with integrating third-parties into a company's business. These risks can be service disruption, regulatory, political, and more recently *Environmental, Social and Governance* (ESG), as well as loss of intellectual property – **and data breach**.

Why **Internal Audit** and Why **Now**

Internal Audit has the traditional role to act as third-line of defense in terms of averting risks to the business, but is also tasked to detect missed opportunities in reaching corporate goals by looking at the enterprise in its entirety. Having the direct communication channel to the CEO and the Board, **Internal Audit** is in the unique position to amplify voices in the organization that otherwise often remain unheard.

Third-Party Risk Management is a process that sits at the juncture of risk and benefit, and until now has widely failed to quantify one of the largest risks to the organization: cumulative third-party data breach risk.

The reason TPRM programs have not quantified this risk is because there has not been a practical way. Recently, statistical models have become available that finally allow this significant risk to be easily quantified and directly managed. These models are accurate for PII data breach and forecast based upon factors that are obvious to even the non-expert: does a company simply have enough trained employees to get the job done. Most importantly, these models generate **probabilities, not scores**, and probabilities allow calculating cumulative-risk.

Interestingly, these models find that **Internal Auditors** (in cybersecurity parlance, the 3rd-line of defense) are very effective at reducing the probability for a data breach. This may come as a surprise because the cybersecurity practice focuses primarily on controls.

With newly discovered value of **Internal Audit** at reducing data breach risk, with new tools finally available to practically and objectively address cumulative third-party data breach risk, with the Board of Directors depending on **Internal Audit** to assure the most effective approaches to protect company value and reach corporate goals, we believe now is the time when **Internal Audit** can shepard a needed change to TPRM that improves effectiveness and allows business to better leverage the value of third-parties.

What is Cumulative Third Party Data Breach Risk

Most companies with mature TPRM programs vet each vendor using maturity scores, SOC 2 reports or their own questionnaires, then use the vendor contract to compel the vendor to address deficiencies in important cybersecurity controls. But it is important to realize that despite your TPRM team's best efforts, the probability that a vendor can have a data breach **is not zero**. The probability for a third-party data breach therefore increases with the number of vendors that could expose your data if they were to have an internal data breach. We will refer to this as **cumulative-probability**.

Cumulative-probability can be calculated as the sum of the probabilities for each vendor. For example, if there were five vendors that could expose data, and the annual probabilities for a data breach were 4%, 3%, 2%, 2% and 1%, then the annual cumulative-probability that one of the companies could experience a data breach would be 12%.

It is important to understand that even if the probability for any particular vendor is insignificant, the cumulative-probability can become significant. Because it is a sum across all vendors that can expose data, cumulative-probability will always be greater than the probability for any single vendor – **and therefore the greatest data breach risk from third-parties**. In the example of the previous paragraph, cumulative-probability is 12%, which is three times greater than the 4% probability for the worst vendor.

Probability for data breach is a strong function of data breach size, with larger data breaches being more rare. In this white paper, we will refer to the consideration of cumulative-probability by data breach size as **cumulative-risk**.

Compliance with Frameworks and Regulation

Internal Audit often likes to reference a basis for beginning an assessment. If obvious ineffectiveness and inefficiency in a process that can impact a company reaching its corporate goals is not a sufficient basis, then consider that current processes for TPRM also fail to be compliant with most frameworks and regulations.

All regulation and most frameworks require consideration of cumulative-risk, even if it is not explicitly stated. For example, COBIT APO 10.04 states “Identify and manage risk relating to vendors’..." where the authors and reviewers understood that there is an aggregate risk which must be *identified* (note the plural-possessive: vendors’). With the word “identified”, the authors are saying this risk cannot just be incidentally managed as current TPRM programs do using questionnaires and scores.

With IaaS and PaaS, third-parties are now an integral part of the I&T-related risks for any enterprise and COBIT APO 12 states “Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.” Here again, risks that threaten tolerance levels must be *identified*, not just incidentally managed.

In the United States, regulation related to Protected Health Information (PHI), 45 CFR 164.308 (a.1.ii.A) states that a risk analysis must be ***accurate*** and thorough. Certainly an analysis which fails to correctly identify the largest risk from third-parties is not accurate. It is important to remember that companies have PHI as part of the HR data which is often hosted in cloud applications.

Regulators in many countries have decided to clearly spell it out. For example in Canada, the Office of the Superintendent of Financial Institutions (OSFI) states in their Third-Party Risk Management Guideline, 2.4.1.2 “...individually and in aggregate…”. If your reaction is: “my company is not in

Canada", consider that the natural laws that govern probability are not different in Canada and that regulators simply had the courtesy to – spell it out.

Protocol

Here we outline simple steps that **Internal Audit** can use to work with the TPRM team to quantify cumulative third-party data breach risk and compare this risk to the likelihood that the company will have an internal data breach (henceforth: **internal-probability** or **internal-risk**). We use a comparison with internal-risk because we find that probabilities for an *internal* data breach can be an objective and accurate proxy for management's risk tolerance.

Making a process complicated does not make it necessarily better, but it does make it difficult to understand and to test. Therefore in designing the steps, we strove for simplicity, while also incorporating observations from statistical modeling of both the probability and financial impact of historical data breaches.

We include an example vendor list in the steps below, and we compare this vendor list to the internal-probabilities for three different enterprises.

Step-1, Obtain a List of Vendors

This step is performed by **Internal Audit**.

From the **Third Party Risk Management** team, obtain a full list of all vendors that could expose your company's PII data in the event that they were to experience a data breach. Data should be any personal information that would require reporting by law (henceforth: PII), including as Protected Health Information (PHI), Card Holder Data (CHD), Personal Financial Information (PFI) and nonpublic Personal Identifiable Information (PII).

As we are only considering a third-party data breach, where data is exposed because the vendor experienced a data breach, you should not include vendors where PII data is encrypted or obfuscated. For example, if there is a database in Amazon Web Services (AWS) that is not encrypted, then include AWS. If the database is encrypted and your company holds the encryption keys, don't include it. If your company sends backups to Iron Mountain, and they are encrypted, don't include Iron Mountain. Do not include vendors that work within your enterprise unless this work includes taking a copy of your PII data into their enterprise. Vendors that work within your company are addressed below in Step-5. Of course, do not include vendors that do not have significant amounts of your PII data. (or per GDPR, e.g. Art. 30 (5): … that do only process personal data "occasionally").

Since the probability of a third-party data breach is cumulative, it is important to obtain a complete list of vendors that can expose your data. In some larger companies, TPRM might be handled by multiple teams, for example, teams in different countries, or different offices. Therefore you might need to work with multiple TPRM teams. TPRM of some vendors might be handled by shadow-IT groups (IT personnel that are embedded within a business group) and it is important to consider these vendors also.

You should consider externally hosted HR systems, externally hosted email, PaaS like Salesforce or Heroku, and IaaS like AWS. You should consider companies that perform transaction processing, external laboratories that might have patient data, call-centers that have your customer data, the company that provides your website, companies that perform fraud monitoring. You should consider hosted file systems that may contain unstructured data. You should consider recorded meetings such as Zoom, where recordings might include PII and where recordings are stored in the cloud. When considering a cloud based system, if it is reasonable that PII could be there and your company does not enforce policies that prohibit PII data, or if there is no evidence that these policies are followed – assume there may be some PII.

For each vendor, also take into account the impact if the vendor were to have a data breach. We will estimate the impact simply by considering the number of people that would need to be notified if the vendor were to experience a data breach (henceforth, **breach-size**). We make this simplification because we know that the correlation between the cost of a data breach and the kind of reportable PII exposed is not statistically significant and that the cost of a data breach increases by the square-root of the number of people affected.

Vendor	People Affected	Vendor	People Affected
Vendor-1	1,000,000	Vendor-17	100,000
Vendor-2	1,000,000	Vendor-18	100,000
Vendor-3	1,000,000	Vendor-19	100,000
Vendor-4	1,000,000	Vendor-20	100,000
Vendor-5	1,000,000	Vendor-21	100,000
Vendor-6	1,000,000	Vendor-22	100,000
Vendor-7	1,000,000	Vendor-23	100,000
Vendor-8	1,000,000	Vendor-24	100,000
Vendor-9	1,000,000	Vendor-25	10,000
Vendor-10	100,000	Vendor-26	10,000
Vendor-11	100,000	Vendor-27	10,000
Vendor-12	100,000	Vendor-28	10,000
Vendor-13	100,000	Vendor-29	10,000
Vendor-14	100,000	Vendor-30	10,000
Vendor-15	100,000	Vendor-31	10,000
Vendor-16	100,000	Vendor-32	10,000

Example list of vendors that could expose reportable PII data if they were to have a data breach. The column labeled ***People Affected*** is the approximate number of people who would need to be notified in the event of a data breach. We have rounded the number affected to the closest breach size that we use in our analysis (i.e. 100+, 1K+, 10K+ etc.). We have not recorded the kind of PII that could be exposed because modeling does not find a statistically significant correlation between the kind of PII data exposed and the cost of a data breach. We have obfuscated vendor names since in the following steps we will show a snapshot in time of the vendor, vendors do sometimes change their security and we do not want to show outdated probabilities for well-known vendors.

Below is an actual vendor list we will use in the following steps to illustrate how to perform the protocol. Vendor names have been obfuscated since this is a point in time analysis, and headcounts and probabilities could be different by the time you read this white paper. The number of people affected has been rounded to the nearest size that we use in our analysis.

Step-2, Send Vendor list to Model-Provider

This step is performed by **Internal Audit**.

Send the vendor list and the number of people that would need to be notified in the event of a third party data breach (potential data breach size), to a company that has access to accurate probability models for PII data breach (**model-provider**[1]). You might need a non-disclosure agreement with the model provider

[1] VivoSecurity in California, Strategic Risk Associates in Virginia USA, IHS Markit (now part of S&P Global).

if your company regards the vendor list as proprietary information, especially when combined with the amount of data that could be exposed.

The steps in this protocol can be executed with any model for the probability of a PII data breach that can be applied to both your vendors and to your company. Here we will describe the steps using an empirical regression model that calculates probabilities based upon the count of employees with certain certifications (henceforth: **certification-headcounts**).

Step-3, Model-Provider Obtains Predictive Factors

This step is performed by the model-provider.

Using only the vendor's name, the model-provider obtains all certification-headcounts. All headcounts are obtained without contacting the vendor.

These certification-headcounts, besides allowing an accurate calculation for the probability of a data breach in step-4, also present a high-level view of the risks from the enterprise and the people-resources brought to bear to reduce this risk. Since you will receive these headcounts, we want to point out their additional value, beyond simply being used to calculate probabilities.

It is important to understand that these predictive factors were discovered through empirical regression modeling and should be considered as statistical facts and not assumptions. But your expert interpretations of these factors can help you understand how effectively the vendor is addressing risk. These certification-headcounts along with example interpretations are presented in the table below.

Predictor	**Description**	**Interpretation**	**Effect on breach probability**
CISSP	Number of employees with the CISSP certification from (ISC)[2]	The 2nd-line of defense	Strong effect, reducing
CISA	Number of employees with the CISA certification from ISACA	The 3rd-line of defense	Strong effect, reducing
MCSA	Number of employees with the Microsoft Certification	Part of the 1st-line of defense. A measure of vendor certification in general. An interest by management in using trained and certified employees.	Modest effect, reducing
RHCE	Number of employees with the Linux Red Hat Certification	An additional technology stack to secure	Modest effect, increasing
Employees	Number of FTE employees	The attack surface. The number of things that can be lost or stolen. An increased probability for a malicious insider	Modest effect, increasing

Note: Predictors in the table were found empirically. The regression model is very accurate, finding orders of magnitude differences between companies. Accuracy can be characterized as identifying 0.4% of companies that will be responsible for 50% of data breaches.

For example, a vendor with a large CISSP-headcount relative to their company size likely has a low risk tolerance and a strong cybersecurity posture. A vendor with a CISA-headcount that is similar in size to their CISSP-headcount likely understands the value of the 3rd-line of defense. A vendor with a larger than normal MCSA-headcount is a company that invests in its 1st-line of defense and emphasizes hiring IT employees that are well trained in the systems they support.

Below is the vendor list from step-1, with certification-headcounts found by the model-provider. To demonstrate the value of interpreting certification-headcounts, we will compare a few vendors in the list.

You can see that vendor-27 with 14 CISSP-certified employees has twice the number as vendor-31 even though these companies are of similar size, and therefore similar risk. Since staffing is one of the major cybersecurity costs, it would appear that vendor-27 has made twice the investment in cybersecurity.

As another example, vendor-30, with 24 CISSP-certified employees has eight times as many as vendor-18, even though these companies are of similar size. In fact, vendor-18 has fewer CISSP-certified employees as vendor-31, even though vendor-18 is much larger. Vendor-30 also invested in a large number of CISA-certified employees and therefore has a strong 3rd-line of defense. Vendor-30's strong security posture is reflected by a low probability for data breach as can be seen in the data in step-4.

			Predictive Headcounts			
Vendor	People Affected	Vendor Employees	RHCE	CISSP	CISA	MCSA
Vendor-1	1,000,000	224	1	1	0	0
Vendor-2	1,000,000	2003	14	56	6	6
Vendor-3	1,000,000	1862	3	90	12	14
Vendor-4	1,000,000	23	0	0	0	0
Vendor-5	1,000,000	110	2	0	0	0
Vendor-6	1,000,000	375	1	3	1	2
Vendor-7	1,000,000	57999	131	250	57	214
Vendor-8	1,000,000	609	0	1	0	1
Vendor-9	1,000,000	23	0	0	0	0
Vendor-10	100,000	3189	5	17	8	6
Vendor-11	100,000	1165	0	2	0	0
Vendor-12	100,000	93	0	0	0	0
Vendor-13	100,000	133	0	0	0	0
Vendor-14	100,000	10834	21	100	21	215
Vendor-15	100,000	10	0	0	0	0
Vendor-16	100,000	444	0	2	1	0
Vendor-17	100,000	30	0	0	0	0
Vendor-18	100,000	3383	6	3	6	4
Vendor-19	100,000	2416	10	14	4	14
Vendor-20	100,000	196781	103	300	150	165
Vendor-21	100,000	1371	0	1	1	1
Vendor-22	100,000	1303	0	0	3	7
Vendor-23	100,000	23	0	0	0	0
Vendor-24	100,000	17	1	0	0	0
Vendor-25	10,000	320	0	1	2	1
Vendor-26	10,000	616	0	0	0	2
Vendor-27	10,000	2312	2	14	3	6
Vendor-28	10,000	423	0	0	0	0
Vendor-29	10,000	123	0	0	0	0
Vendor-30	10,000	3833	2	24	19	3
Vendor-31	10,000	2684	1	7	3	0
Vendor-32	10,000	107	1	0	0	0

Example list of vendors from step-1, now with certification-headcounts found for each vendor. This information was obtained by the model-provider from public sources and will be used to calculate probabilities for each vendor. This information already provides much information about the vendors' security postures. For example, you can see that Vendor-30 has twice the number of CISSP certified cybersecurity employees as Vendor-31 even though these vendors have similar numbers of employees.

The aim of this protocol is simply to determine if third-party data breach risk is within management's risk tolerance. But **Internal Audit** could go further and compare individual assessments made by the TPRM team using traditional methods with observations made based upon certification-headcounts, to determine if the observations made by traditional methods are justified.

If it seems unreasonable not to look at cybersecurity controls, consider that you might be missing the forest for the trees. Empirical modeling finds that the number of trained and certified people greatly reduces the probability for a data breach. Indeed, it is these very people who are continually assessing risk, then deploying and monitoring the controls that you are looking for in traditional methods for TPRM. If you find a gap in cybersecurity controls, assuming that the control is indeed effective at reducing data breach, then modeling suggests that not having enough of the right people is the likely root cause of the control-gap.

Step-4, Model-Provider Calculates Probabilities

This step is performed by the model-provider.

Using the predictive factors from Step-3, the model provider calculates data breach probability broken down by data breach size (number of people affected), for each vendor.

Vendor	People Affected	Employees	RHCE	CISSP	CISA	MCSA	1+	10+	100+	1,000+	10,000+	100,000+	1,000,000+	10,000,000+	100,000,000+
Vendor-1	1,000,000	224	1	1	0	0	0.34%	0.34%	0.33%	0.27%	0.12%	0.0495%	0.0149%	0.001506%	0.000244%
Vendor-2	1,000,000	2003	14	56	6	6	0.87%	0.86%	0.56%	0.21%	0.02%	0.0023%	0.0002%	0.000003%	0.000000%
Vendor-3	1,000,000	1862	3	90	12	14	0.11%	0.11%	0.05%	0.01%	0.00%	0.0000%	0.0000%	0.000000%	0.000000%
Vendor-4	1,000,000	23	0	0	0	0	0.03%	0.03%	0.03%	0.02%	0.01%	0.0049%	0.0016%	0.000171%	0.000029%
Vendor-5	1,000,000	110	2	0	0	0	9.88%	9.91%	9.74%	8.42%	4.23%	1.8571%	0.6157%	0.072820%	0.013075%
Vendor-6	1,000,000	375	1	3	1	2	0.05%	0.05%	0.04%	0.03%	0.01%	0.0019%	0.0004%	0.000019%	0.000002%
Vendor-7	1,000,000	57999	131	250	57	214	28.15%	28.25%	27.57%	23.00%	10.48%	4.2385%	1.2859%	0.132337%	0.021639%
Vendor-8	1,000,000	609	0	1	0	1	0.22%	0.22%	0.21%	0.18%	0.09%	0.0357%	0.0112%	0.001215%	0.000206%
Vendor-9	1,000,000	23	0	0	0	0	0.03%	0.03%	0.03%	0.02%	0.01%	0.0049%	0.0016%	0.000171%	0.000029%
Vendor-10	100,000	3189	5	17	8	6	0.75%	0.76%	0.71%	0.52%	0.17%	0.0521%	0.0119%	0.000790%	0.000096%
Vendor-11	100,000	1165	0	2	0	0	1.47%	1.48%	1.45%	1.26%	0.64%	0.2809%	0.0937%	0.011179%	0.002019%
Vendor-12	100,000	93	0	0	0	0	0.16%	0.16%	0.16%	0.14%	0.07%	0.0305%	0.0100%	0.001179%	0.000211%
Vendor-13	100,000	133	0	0	0	0	0.25%	0.26%	0.25%	0.22%	0.11%	0.0485%	0.0162%	0.001932%	0.000349%
Vendor-14	100,000	10834	21	100	21	215	2.18%	2.19%	2.11%	1.68%	0.68%	0.2500%	0.0684%	0.005996%	0.000880%
Vendor-15	100,000	10	0	0	0	0	0.01%	0.01%	0.01%	0.01%	0.00%	0.0017%	0.0005%	0.000054%	0.000009%
Vendor-16	100,000	444	0	2	1	0	0.14%	0.14%	0.14%	0.11%	0.04%	0.0142%	0.0037%	0.000299%	0.000042%
Vendor-17	100,000	30	0	0	0	0	0.04%	0.04%	0.04%	0.03%	0.02%	0.0070%	0.0022%	0.000246%	0.000042%
Vendor-18	100,000	3383	6	3	6	4	1.87%	1.88%	1.79%	1.37%	0.51%	0.1734%	0.0439%	0.003415%	0.000463%
Vendor-19	100,000	2416	10	14	4	14	0.89%	0.89%	0.86%	0.68%	0.27%	0.0961%	0.0257%	0.002174%	0.000312%
Vendor-20	100,000	196781	103	300	150	165	69.45%	69.61%	68.85%	61.18%	33.47%	15.8246%	5.6873%	0.763804%	0.149409%
Vendor-21	100,000	1371	0	1	1	1	0.36%	0.36%	0.35%	0.29%	0.13%	0.0535%	0.0162%	0.001663%	0.000271%
Vendor-22	100,000	1303	0	0	3	7	0.64%	0.64%	0.63%	0.54%	0.26%	0.1136%	0.0368%	0.004203%	0.000737%
Vendor-23	100,000	23	0	0	0	0	0.03%	0.03%	0.03%	0.02%	0.01%	0.0049%	0.0016%	0.000171%	0.000029%
Vendor-24	100,000	17	1	0	0	0	28.65%	28.74%	28.13%	23.77%	11.22%	4.6702%	1.4619%	0.157996%	0.026699%
Vendor-25	10,000	320	0	1	2	1	0.02%	0.02%	0.02%	0.01%	0.00%	0.0004%	0.0001%	0.000003%	0.000000%
Vendor-26	10,000	616	0	0	0	2	0.50%	0.50%	0.49%	0.43%	0.23%	0.1059%	0.0370%	0.004753%	0.000902%
Vendor-27	10,000	2312	2	14	3	6	0.44%	0.45%	0.42%	0.32%	0.11%	0.0373%	0.0091%	0.000672%	0.000088%
Vendor-28	10,000	423	0	0	0	0	1.05%	1.05%	1.04%	0.91%	0.48%	0.2174%	0.0751%	0.009477%	0.001778%
Vendor-29	10,000	123	0	0	0	0	0.23%	0.23%	0.23%	0.20%	0.10%	0.0438%	0.0146%	0.001734%	0.000313%
Vendor-30	10,000	3833	2	24	19	3	0.68%	0.69%	0.61%	0.39%	0.10%	0.0239%	0.0044%	0.000205%	0.000020%
Vendor-31	10,000	2684	1	7	3	0	1.55%	1.56%	1.51%	1.21%	0.50%	0.1885%	0.0527%	0.004767%	0.000715%
Vendor-34	10,000	107	1	0	0	0	18.30%	18.35%	18.05%	15.59%	7.83%	3.4335%	1.1374%	0.134345%	0.024101%

Example list of vendors from step-2, now with probabilities calculated for each vendor by the model-provider, based upon certification-headcounts. Probabilities are for indicated data breach sizes that the vendor could experience, where 1+ should be read as 1-person or more affected, 10+ means 10-people or more affected. The table shows that there are many orders of magnitude differences between vendors, and generally companies with a large number of employees have a higher probability for data breach.

Step-5, Model-Provider Calculates Cumulative-Probabilities

This step is performed by the model-provider but it can also be performed by **Internal Audit**.

In step-4, the model-provider calculated probabilities for each vendor to have a data breach for a range of size. The breach sizes are sizes for the vendors, not sizes for your organization. For each vendor, the model provider must now find a data breach size that the vendor could experience, that is so large that it could include your organization's data.

For example, vendor-31 has 10,000 of your records, but this vendor has records from many other customers, too. The model provider must therefore find a data breach size being so large that it would include your organization's 10,000-records along with other customers' data. Such a determination can be based on the amount of data that can be exposed for your company and the size of the vendor, with larger vendors having more customers and therefore requiring a larger data breach size to expose your data. In the case of vendor-31, a data breach affecting 1-million people was determined to be large enough to include your 10,000-records. The probability for vendor-31 having a data breach affecting 1-million people is 0.053% annually and this will be the probability used for exposing your 10,000-records through vendor-31.

The model-provider repeats this process for each vendor.

				Vendor's Breach Size and Probabilites								
Vendor	People Affected	My Probabilites	Vendor Employees	1+	10+	100+	1,000+	10,000+	100,000+	1,000,000+	10,000,000+	100,000,000+
Vendor-1	1,000,000	0.002%	224	0.34%	0.34%	0.33%	0.27%	0.12%	0.0495%	0.0149%	0.002%	0.000244%
Vendor-2	1,000,000	0.000003%	2003	0.87%	0.86%	0.56%	0.21%	0.02%	0.0023%	0.0002%	0.000003%	0.000000%
Vendor-3	1,000,000	0.00000001%	1862	0.11%	0.11%	0.05%	0.01%	0.00%	0.0000%	0.0000%	0.000000%	0.000000%
Vendor-4	1,000,000	0.0002%	23	0.03%	0.03%	0.03%	0.02%	0.01%	0.0049%	0.0016%	0.0002%	0.000029%
Vendor-5	1,000,000	0.07%	110	9.9%	9.9%	9.7%	8.4%	4.2%	1.9%	0.62%	0.07%	0.013075%
Vendor-6	1,000,000	0.00002%	375	0.05%	0.05%	0.04%	0.03%	0.01%	0.0019%	0.0004%	0.00002%	0.000002%
Vendor-7	1,000,000	0.13%	57999	28%	28%	28%	23%	10%	4.2%	1.3%	0.13%	0.021639%
Vendor-8	1,000,000	0.001%	609	0.22%	0.22%	0.21%	0.18%	0.09%	0.0357%	0.0112%	0.001%	0.000206%
Vendor-9	1,000,000	0.0002%	23	0.03%	0.03%	0.03%	0.02%	0.01%	0.0049%	0.0016%	0.0002%	0.000029%
Vendor-10	100,000	0.01%	3189	0.75%	0.76%	0.71%	0.52%	0.17%	0.0521%	0.01%	0.000790%	0.000096%
Vendor-11	100,000	0.09%	1165	1.47%	1.48%	1.45%	1.26%	0.64%	0.2809%	0.09%	0.011179%	0.002019%
Vendor-12	100,000	0.01%	93	0.16%	0.16%	0.16%	0.14%	0.07%	0.0305%	0.01%	0.001179%	0.000211%
Vendor-13	100,000	0.02%	133	0.25%	0.26%	0.25%	0.22%	0.11%	0.0485%	0.02%	0.001932%	0.000349%
Vendor-14	100,000	0.01%	10834	2.2%	2.2%	2.1%	1.7%	0.68%	0.25%	0.0684%	0.005996%	0.000880%
Vendor-15	100,000	0.001%	10	0.01%	0.01%	0.01%	0.01%	0.00%	0.0017%	0.001%	0.000054%	0.000009%
Vendor-16	100,000	0.004%	444	0.14%	0.14%	0.14%	0.11%	0.04%	0.0142%	0.004%	0.000299%	0.000042%
Vendor-17	100,000	0.002%	30	0.04%	0.04%	0.04%	0.03%	0.02%	0.0070%	0.002%	0.000246%	0.000042%
Vendor-18	100,000	0.04%	3383	1.87%	1.88%	1.79%	1.37%	0.51%	0.1734%	0.04%	0.003415%	0.000463%
Vendor-19	100,000	0.03%	2416	0.89%	0.89%	0.86%	0.68%	0.27%	0.0961%	0.03%	0.002174%	0.000312%
Vendor-20	100,000	0.15%	196781	69%	70%	69%	61%	33%	16%	5.7%	0.8%	0.15%
Vendor-21	100,000	0.02%	1371	0.36%	0.36%	0.35%	0.29%	0.13%	0.0535%	0.02%	0.001663%	0.000271%
Vendor-22	100,000	0.04%	1303	0.64%	0.64%	0.63%	0.54%	0.26%	0.1136%	0.04%	0.004203%	0.000737%
Vendor-23	100,000	0.002%	23	0.03%	0.03%	0.03%	0.02%	0.01%	0.0049%	0.002%	0.000171%	0.000029%
Vendor-24	100,000	1.46%	17	29%	29%	28%	24%	11%	4.6702%	1.46%	0.157996%	0.026699%
Vendor-25	10,000	0.0004%	320	0.02%	0.02%	0.02%	0.01%	0.00%	0.0004%	0.0001%	0.000003%	0.000000%
Vendor-26	10,000	0.11%	616	0.50%	0.50%	0.49%	0.43%	0.23%	0.11%	0.0370%	0.004753%	0.000902%
Vendor-27	10,000	0.01%	2312	0.44%	0.45%	0.42%	0.32%	0.11%	0.0373%	0.01%	0.000672%	0.000088%
Vendor-28	10,000	0.22%	423	1.05%	1.05%	1.04%	0.91%	0.48%	0.22%	0.0751%	0.009477%	0.001778%
Vendor-29	10,000	0.04%	123	0.23%	0.23%	0.23%	0.20%	0.10%	0.04%	0.0146%	0.001734%	0.000313%
Vendor-30	10,000	0.004%	3833	0.68%	0.69%	0.61%	0.39%	0.10%	0.0239%	0.004%	0.000205%	0.000020%
Vendor-31	10,000	0.053%	2684	1.55%	1.56%	1.51%	1.21%	0.50%	0.1885%	0.053%	0.004767%	0.000715%
Vendor-32	10,000	3.43%	107	18%	18%	18%	16%	7.8%	3.43%	1.1374%	0.134345%	0.024101%

Example vendor list from step-3, now with probabilities chosen (My Probabilities column) for each vendor that are considered large enough to include your records (highlighted in yellow).

With a data breach size and associated probabilities found for each vendor, the model-provider now calculates cumulative-probabilities for each third-party breach size that your company can experience. For example, the figure shows that summing the eight probabilities for vendors that have 10K of your records comes to a 4% probability.

Vendor	People Affected	My Probabilites	Cumulative Probabilities
Vendor-1	1,000,000	0.002%	
Vendor-2	1,000,000	0.000003%	
Vendor-3	1,000,000	0.00000001%	
Vendor-4	1,000,000	0.0002%	
Vendor-5	1,000,000	0.07%	**Sum~0.2%**
Vendor-6	1,000,000	0.00002%	
Vendor-7	1,000,000	0.13%	
Vendor-8	1,000,000	0.001%	
Vendor-9	1,000,000	0.0002%	
Vendor-10	100,000	0.01%	
Vendor-11	100,000	0.09%	
Vendor-12	100,000	0.01%	
Vendor-13	100,000	0.02%	
Vendor-14	100,000	0.01%	
Vendor-15	100,000	0.001%	
Vendor-16	100,000	0.004%	
Vendor-17	100,000	0.002%	**Sum~2%**
Vendor-18	100,000	0.04%	
Vendor-19	100,000	0.03%	
Vendor-20	100,000	0.15%	
Vendor-21	100,000	0.02%	
Vendor-22	100,000	0.04%	
Vendor-23	100,000	0.002%	
Vendor-24	100,000	1.46%	
Vendor-25	10,000	0.0004%	
Vendor-26	10,000	0.11%	
Vendor-27	10,000	0.01%	
Vendor-28	10,000	0.22%	**Sum~4%**
Vendor-29	10,000	0.04%	
Vendor-30	10,000	0.004%	
Vendor-31	10,000	0.053%	
Vendor-32	10,000	3.43%	

Example vendor list from step-3, with a chosen probability for each vendor (My Probabilities column), now summed for each data breach size (People Affected column), to calculate cumulative-probabilities. Our annual cumulative-probabilities are therefore 4% for a data breach affecting 10-thousand people, 2% for a data breach affecting 100-thousand people and 0.2% for a data breach affecting 1-million people.

Step-6, Work with Model-Provider to obtain Internal-Probabilities

This step is performed by the model-provider, with the assistance of **Internal Audit**.

In this step, an objective standard is created to compare your company's cumulative-probabilities. This standard will be the probability that your company can experience a data breach internally (henceforth: **internal-probabilities**). To obtain internal-probabilities, the model-provider applies the model directly to your company and calculates probabilities based upon your company's certification-headcounts.

These internal-probabilities will serve as an objective measure of your management's risk tolerance because your company's certification-headcounts reflect the amount of money your company spends on staffing levels, which is one of the largest cybersecurity costs. These staffing levels also naturally capture the man-power your company puts into continually assessing risk, deploying and monitoring controls.

These staffing levels also reflect the emphasis your company puts into the three lines of defense (see table in step-3).

Begin by asking the model provider to assess your company, and to supply the names of the people within your organization with the certifications used as predictive factors. These people will generally work in departments as indicated in the following table. You should work with these departments to verify headcounts and determine if any certifications were missed.

Certification	Departments
CISSP	Cybersecurity, TPRM
CISA	Internal Audit, Cybersecurity, TPRM, Compliance, Legal
MCSA	IT, shadow-IT
RHCE	IT, shadow-IT

Departments where certified employees can be found. Verify the headcounts given to you by the model-provider and determine if certification employees were missed.

Also, work with the model provider to obtain an accurate assessment of the number of employees with access to your enterprise resources. This should include all full-time employees (FTE), all part-time employees (PTE) and contractors. Part-time employees can be included in the model as 50% of a FTE.

After headcounts are verified and corrected, the model-provider calculates internal-probabilities for your company.

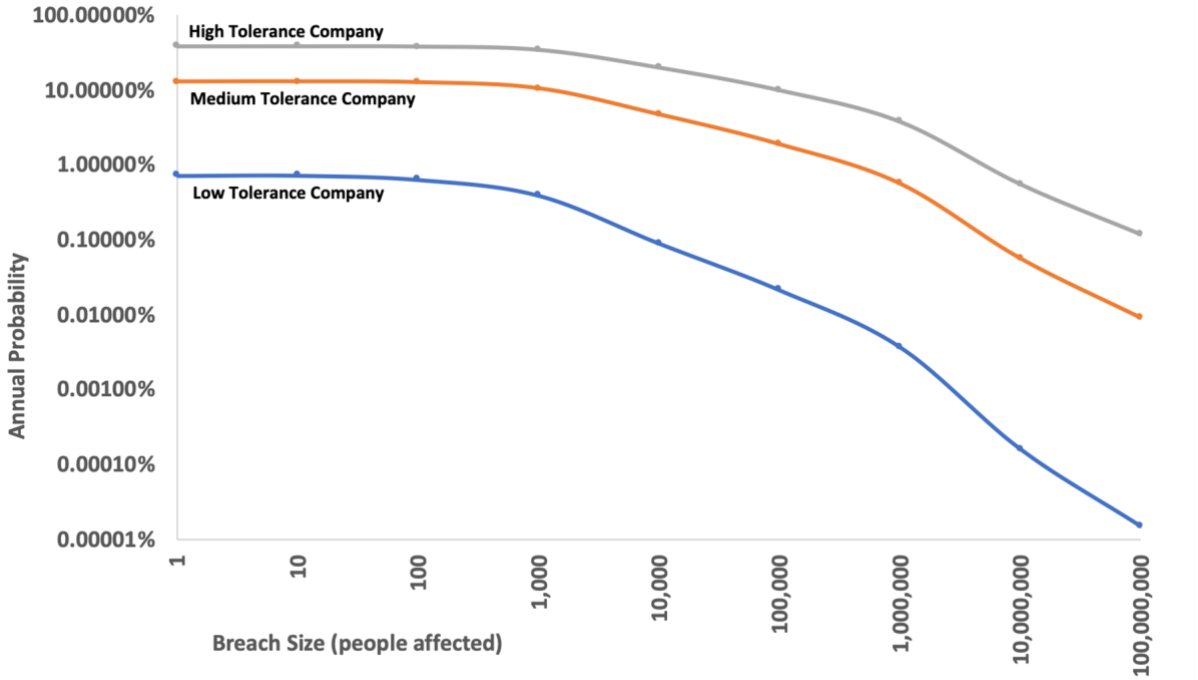
Step-7, Compare Cumulative-Probabilities with Internal-Probabilities

This step is performed by **Internal Audit**.

With results received back from the model-provider, **Internal Audit** is now ready to compare cumulative-probability with internal-probabilities and objectively assess the effectiveness of the TPRM process for maintaining third-party data breach risk within executive management's risk tolerance.

To illustrate how to perform this comparison, we have calculated internal-probabilities for three companies, and we pose these probabilities as your internal-probabilities. These are real and well-known companies that represent a large range in risk-tolerance and will allow you to see the range of observations you might make. Because headcounts and probabilities represent only a point in time assessment, we have obfuscated their names and we will refer to them simply as the **High Tolerance**, **Medium Tolerance** and **Low Tolerance Company**.

The graph and table below compares these companies and show very large differences for the probability of a data breach and corresponding cybersecurity investments. It is clear from the table that the **High Tolerance Company** has made a factional investment into all three lines of defense, compared with the **Medium Tolerance Company** and has a much higher probability for a data breach across all data breach



Probabilities for three example companies which we will pose as your company in the examples below. These companies are identified as low, medium and high risk tolerance. The Y-axis is the annual probability for a PII data breach and the X-axis is data breach size, where 1 means 1 or more people affected, 10 means 10 or more people affected etc. The X and Y-axis are log scales which visually diminishes the large differences between companies. Since these probabilities are based upon headcounts which represent a major portion of cybersecurity-spending for these companies, it is reasonable to assume that these probabilities reflect the risk tolerance of executive management.

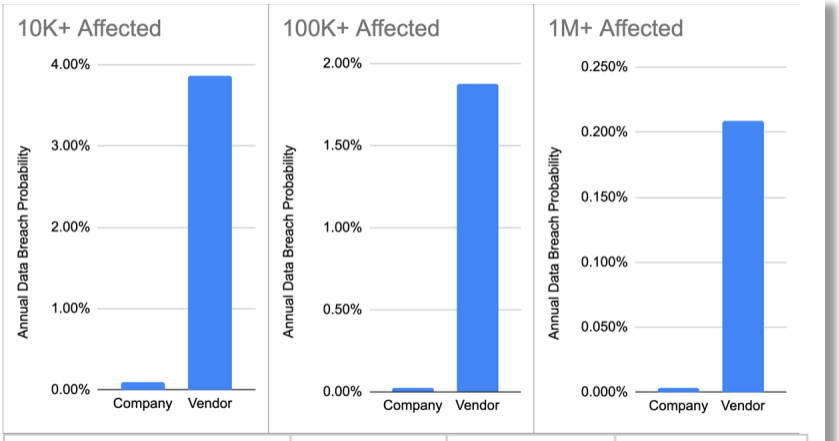
Company	Employees	CISA (% of IT)	CISSP (% of IT)	MCSA (% of IT)
High Tolerance Company	30,504	12 (0.24%)	8 (0.16%)	17 (0.34%)
Medium Tolerance Company	25,106	35 (1.1%)	87 (2.7%)	54 (1.7%)
Low Tolerance Company	2,321	7 (3.1%)	16 (7.2%)	7 (3.1%)

Predictive factors for the three example companies in the graph above. These are headcounts for actual well-known companies, but company names have been obfuscated since these reflect a moment in time and might not reflect the companies today. Numbers within parentheses are the headcounts normalized by the size of IT.

sizes. The **Low Tolerance Company** has made an order of magnitude greater investment for their size, and has more than three orders of magnitude lower probability for a large data breach compared with the **High Tolerance Company**. In fact, the **Low Tolerance Company** has twice the number of CISSP-certified employees compared with the **High Tolerance Company** even though they have less than one-tenth the number of employees.

Low Tolerance Company

We begin by comparing cumulative-probabilities of the vendor list from step-5 with the internal-probabilities of the **Low Tolerance Company**. Note that we have rounded vendor breach sizes in step-5 to the closest sizes that match the breach sizes for internal-probabilities, which leaves breach sizes 10K+, 100K+ and 1M+ affected. Comparing the internal-probability and cumulative-probability rows in the table, we can see that cumulative-probability is 40, 100 and 50-times larger than internal-probabilities for 10K+, 100K+ and 1M+ affected respectively. The bar-graphs are provided to show this large difference, visually.



	10,000+	100,000+	1,000,000+
Internal-probability	0.09%	0.02%	0.004%
Cumulative-probability	4%	2%	0.2%

Example, the Low Tolerance Company. The table and graphs show that internal-probability represents just 2% of cumulative-probability for breach sizes 10K+ and 1M+ affected and an even small proportion of 1% for 100K+ affected. Any increase or decrease in internal-probability would make little difference since probability for a data breach is dominated by cumulative-probability. Internal Audit should consider that TPRM is undermining the investments made in internal security and TPRM is not managing third party data breach risk within senior management's tolerance levels.

When comparing these probabilities, consider that internal-probabilities are the result of the large investment this company is making in cybersecurity every year. Regarding CISSP and CISA headcounts alone, this small company is spending more than $2M-annually on salaries (based on US-level) and this does not include all the money spent in addition on cybersecurity controls deployed and monitored by the staff of 16 CISSP-certified employees. The low internal-probabilities reflect management's low risk tolerance and are the probabilities this company is expecting from these investments. But these investments are being undermined by TPRM because any substantial increases or decreases in internal cybersecurity spending would have little effect on the probability for a data breach, since probabilities are dominated by cumulative-probabilities.

As a rule of thumb, internal-probabilities should be of similar size or larger than cumulative-probabilities for TPRM to be managing third-party data breach risk within management's risk tolerance and not undermining internal cybersecurity investments.

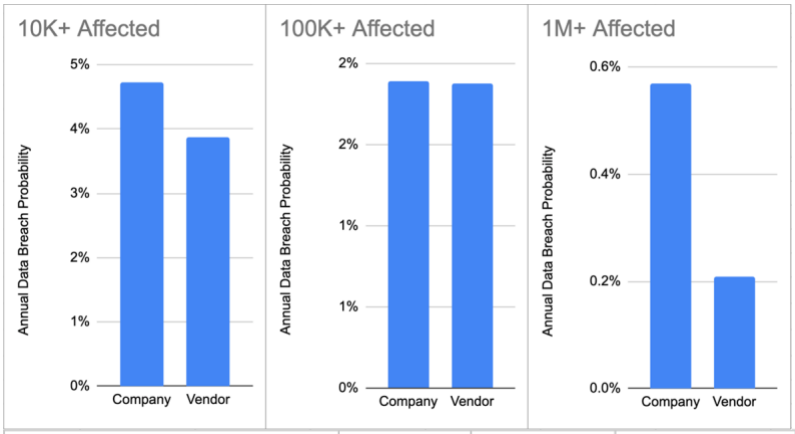
Recommendations

- **Internal Audit** should work with TPRM to consider cumulative-probabilities going forward, since identification of this risk is required by most regulations and frameworks.
- **Internal Audit** should work with TPRM to develop strategies for reducing and maintaining cumulative-risk within management's risk tolerance. Strategies could include: 1) encrypting or obfuscating data shared with the highest risk third-parties, 2) consolidating vendors that offer similar services and thereby reducing the number of vendors overall, 3) requiring a more robust security posture from problem vendors by increasing certified-headcount.
- TPRM should modify procedures to implement strategies.

Medium Tolerance Company

Next, we compare cumulative-probabilities from the vendor list from step-5, with the internal-probabilities of the **Medium Tolerance Company.**

In the table you can see that, for the same vendor list, cumulative-probabilities are similar to internal-probabilities for the **Medium Tolerance Company**. This is due in part to the larger company size and the smaller investment this company has made in cybersecurity in proportion to their size. In this case, it would appear that TPRM is managing third-party data breach risk within management's risk tolerance. TPRM is not undermining internal security investments since a significant change in spending on internal cybersecurity could have a significant effect on the overall probability for a data breach.



	10,000+	100,000+	1,000,000+
Internal-probability	5%	2%	0.6%
Cumulative-probability	4%	2%	0.2%

Example, the Medium Tolerance Company. The table and graphs show that cumulative-probability and internal-probability are very similar. Any increase or decrease to either internal-probability or cumulative-probability would significantly affect probability for a data breach. It seems reasonable to conclude that TPRM is managing third-party data breach within senior management's tolerance level.

Although overall management of third-party data breach risk is within management's risk tolerance, we recommend that **Internal Audit** go further and compare model-based assessments with TPRM assessments for individual vendors as explained in step-3. Given that the model-based forecasts are accurate, we would expect assessments based upon questionnaires and maturity scores to also identify higher risk vendors.

Recommendations

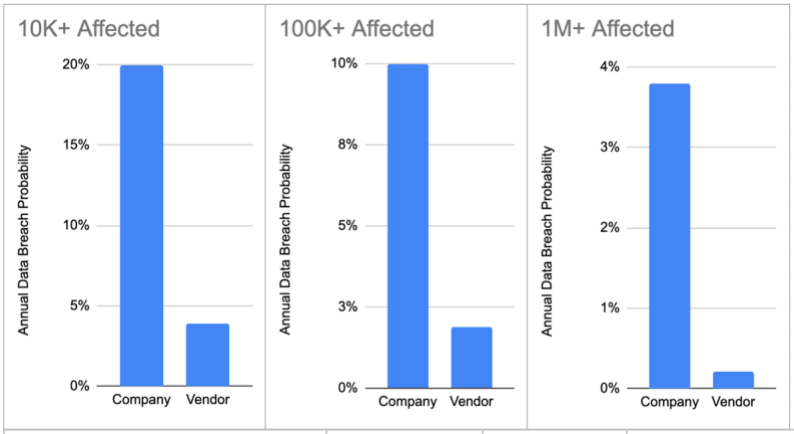
- **Internal Audit** should work with TPRM to consider cumulative-probabilities going forward, since identification of this risk is required by most regulations and frameworks.
- **Internal Audit** should further investigate if the same highest risk vendors are identified using two approaches: questionnaires and regression models.

High Tolerance Company

Finally, we compare cumulative-probabilities from the vendor list from step-5, with the internal-probabilities of the **High Tolerance Company.**

The table shows that cumulative-probabilities are much smaller than internal-probabilities for the **High Tolerance Company** and well within management's risk tolerance.

But perhaps TPRM is hurting the company in a different way: limiting the ability to leverage the value from third-parties. From the table, one can see that internal-probabilities are five-times higher for 10K+ and 100K+ affected and twenty-times higher for 1M+ affected. Relaxing TPRM would likely produce only a small change in the probability for a data breach since the probability is dominated by internal-probabilities. We recommend further investigating if TPRM is hindering the company's ability to leverage the value from third-parties.



	10,000+	100,000+	1,000,000+
Internal-probability	20%	10%	4%
Cumulative-probability	4%	2%	0.2%

Example, the High Tolerance Company. The table and graphs show that cumulative-probability represents 20% of internal-probability for breach sizes 10K+ and 100K+ and an even small proportion of 5% for 1M+ affected. Any increase or decrease in cumulative-probability would make little difference since probability for a data breach is dominated by internal-probability. Internal Audit should consider that TPRM may be limiting the companies about to leverage the use of third-parties.

Recommendations

- **Internal Audit** should work with TPRM to consider cumulative-probabilities going forward, since identification of this risk is required by most regulations and frameworks.
- **Internal Audit** should poll management to determine if TPRM is limiting the company's ability to use third-parties. For example, is it taking too long to on-board new vendors or are vendors being disqualified that the business would like to use. Is data sharing blocked, that could provide significant value?

Step-8 Working with the Management of the Audited Business Unit

The TPRM team may only have ever looked at the problem from the perspective of **impact** to the company and a checklist of controls. However, following broadly acknowledged concepts of risk assessment, senior managers of the TPRM team should also remember that risk is a function of impact **and probability**, so the reintroduction of probability into third-party risk management should come as no surprise. The use of **cumulative** probability may first run against human intuition, therefore we added the section "throwing dice" further below, demonstrating how you can teach yourself (and others) in a playful but compelling way that the principle of cumulative-probability is mathematically correct.

Still there may be a learning curve on how to use this new way to reach and maintain management's risk tolerance levels and apply it to vendor due-diligence and vendor-contracts. Measuring and managing

cumulative vendor risk might require changes to the organizational structure and staffing - and it will certainly require writing new policies and procedures.

Begin by sharing your report with the managers of the TPRM team, with an aim toward working out a mutually agreed upon plan that can be taken to the Board.

Remember, the Board and CEO would rather hear solutions.

Explaining results first to someone familiar with statistics might be helpful as this person can help champion the new approach, otherwise the time to "throw dice" may be well invested.

You might recommend that members of the TPRM team receive training in how to use this new approach before applying it in practice. The TPRM team will view managing cumulative-risk as elevating their role in the company through a clearer understanding of the risk that they manage and by their efforts empowering the business through a smarter use of third-parties.

Step-9 Presenting to the CEO and the Board[2]

More likely, the Board of Directors has only ever viewed cybersecurity from the perspective of green-yellow-red juxtaposed with a diagram of enterprise controls. It will also take time for the Board to understand that the expected frequency of data breach can be known, how to think about this risk and the role they can play in managing this risk.

In presenting to the Board, begin by finding an influencer or champion who will attend the presentation to the Board, and who can advocate for the results and give other Board members confidence. Meet with this person separately well before the Board meeting, explain the findings and present the solution. Just as with the TPRM team, look for a champion who has some understanding of statistics.

Senior managers of the TPRM team should be invited to present their solution to the Board. Of course a winner-loser scenario should be avoided and potential differences regarding the assessment of findings should focus on the matter at hand, not on people.

Throwing dice

Understanding random events can be challenging, even for very smart people. We can all be fooled by the *hot-hand fallacy* or the *gambler's fallacy* - and the research is robust on how experts can be fooled into believing that they are doing the right thing regarding rare events – and data breaches are rare events.

We, the authors, hope this white-paper has demonstrated that assessing third-party risks properly is everything else but a child's game. However, who will say "no" to an easy-to-follow analogy that even injects some fun to the business if it can help to have a more comprehensive understanding of a complex matter such as risk exposure? So we "take the risk" of explaining cumulative-probability by throwing dice. We have found board member to be surprisingly tolerant of game playing activities that help with understanding.

Take the following analogy: a die represents a vendor that you entrusted your PII, each roll represents a year, rolling a "one" represents a data breach.

- Roll a single die multiple times and record the results.

[2] Auditors may instead report to an Audit Committee where organizations are legally obligated or have chosen to establish such a committee in order to discharge the Board's responsibilities. An Audit Committee comprises selected Board members and senior stakeholders. For ease of reading, we here simply refer to the Board.

Considering there are six faces, the probability for a "one" is one-in-six or 16.7%. On average, a "one" should occur every six rolls. In reality, sometimes a "one" occurs several rolls in a row, other times a "one" does not occur even after twenty rolls. But the probability is always 16.7% for each roll (and your result records will show that with an increasing number of rolls you approach having a "one" in 16.7% of the total of rolls).

Considering the initially made representations, this translates to: "The probability for a data breach is one-in-six or 16.7%. On average, a data breach should occur every six-years. In reality, sometimes a data breach occurs several years in a row, other times a data breach does not occur even after twenty years." In the latter case, one can easily be fooled into believing probability is much lower than 16.7% and that our traditional efforts to prevent a data breach are working. "But the probability for a data breach is always 16.7% for each year."

- Now roll three dice simultaneously for multiple times and record the results.

  Given the above explanations for a single die, the probability for a "one" on any of the three dice being rolled simultaneously is three times 16.7% or 50%, i.e. on average, a "one" should occur every two rolls.

  Translation: Having three vendors with a data breach probability of 16.7% for each year will result in a 50% probability of a data breach for your organization in any given year.

One thing to notice in the game playing, when there is just one vendor (one die) and the probability is just 16.7%, there is much more variability than when there are three vendors (three dice) and the probability is 50%. This is called the Law of Large Numbers and it is this variability that makes cybersecurity and assessing risk so challenging.

About the Authors

Axel Troike

With over 20 years of management experience, Axel Troike provides consulting services at the intersection of compliance, business and IT. In recent mandates, Axel has focused on his specialized expertise in conducting assessments of how processing activities and data transfers impact compliance with data protection regulations such as the EU's GDPR.

Previous experiences include leading roles in developing IT-audit guidelines, performing audits of the structural and process organization in application development as well as implementing measures to mitigate identified risks and to optimize efficiency.

Axel has conducted more than 100 projects in 8 countries advising client enterprises regarding the organizational and conceptual aspects of Data Governance, Data Privacy, Master Data Management, Data Strategy, Data & Process Modeling and related topics. He is also President at Grandite in Quebec (Canada), the supplier of the SILVERRUN Business Architecture Tools.

Axel holds a Master's Degree in Mathematics from Christian-Albrechts-University in Kiel, Germany. He can be contacted via Linkedin.

David Hann

David is the director of the UK based **DHann Consulting** which partners with organisations to tackle diverse and complex challenges, from transforming processes and implementing systems, to assessing risk and helping drive organisational change.

David has over twenty-six years of experience in risk, audit, and consulting within the UK and overseas. His experience is founded on a 12-year career focused on Technology Risk at PwC (UK), Deloitte (Australia), and KPMG (Australia), followed by 7-years at Lloyds Banking Group (UK) where he held several 'Head of Audit' roles including Retail Banking Technology, Digital Banking and Telephone Banking. David's focus moved to concentrate on third-party and risk and regulatory compliance. As a regional product director at IHS Markit, he helped to successfully launch one of the world's first third-party risk management due diligence utilities. He subsequently went on to assist clients in implementing solutions to manage their third-party and outsourcing regulatory obligations.

His most recent consulting successes include managing Third-Party Risk programmes, including delivering a global Cyber Security transformation, and implementing a global Third-Party Risk framework. Projects have also included managing part of a multimillion-pound post-merger integration programme in financial services and internal audit assessments at leading digital banks in the UK. David holds a degree in Physics from the University of Southampton. David can be contacted at david@dhannconsulting.com and Linkedin

Thomas Lee

Dr. Thomas Lee is the CEO of VivoSecurity, a Silicon Valley based company focused on data collection, regression modeling and A.I. to bring predictability to the randomness of data breach. In cybersecurity, Thomas has developed models to forecast fraud in online banking, forecast data breach costs and probability for lawsuits in the event of a PII data breach. He has developed models to forecast PII data breaches by state and models to forecast the number of data breaches in the healthcare industry and probability of a PII data breach for companies and third-parties. Thomas has been an invited speaker at the Richmond Fed research conference 2018, invited participant at Richmond Fed cyber security workshop 2019, invited speaker at O.R.X Toronto & Milan 2018, speaker at OpRisk North America 2018, ACAMS panelist 2019, PRMIA NYC & BCG 2018, invited speaker at WiCyS Silicon Valley chapter in 2022, and ISACA Silicon Valley chapter in 2022.

Outside of cybersecurity, Thomas has pioneered computational techniques in medicine for refining x-ray diffraction data, noise reduction in electron micrographs using in 2D Fourier filtering, and singular value decomposition applied to electron micrographs to determine molecular packing of hemoglobin molecules in sickle cell anemia. In the industrial controls industry, he has pioneered pattern matching in the Fourier domain for particle size analysis and pattern matching for acoustic range finders. Thomas has multiple patents and publications in peer reviewed journals and holds BS degrees in Physics and Electrical Engineering from the University of Washington, and an MS and PhD in Biophysics from the University of Chicago. Thomas can be contacted at ThomasL@VivoSecurity.com and on Linkedin.