How to Improve Third-Party Risk Management Using Statistical Models

David Hann
DHann Consulting
David@DHannConsulting.com

Thomas Lee, PhD
VivoSecurity
ThomasL@VivoSecurity.com

Abstract

Third-party risk may account for as much as half of an organization's *operational* risk, yet ***Third-Party Risk Management*** (TPRM) is typically not resourced at the level of non-third-party risks. We believe TPRM is under-resourced because the true magnitude of this risk is not well understood.

In this white paper, we will describe current practice for TPRM and how it can be improved by incorporating **cumulative risk**—the risk from the sheer number of vendors, using statistical models. These improvements will not only increase the effectiveness of TPRM programs at reducing risk, but also quantify this risk in terms that corporate leadership can act upon. It will justify an increase in resources commensurate with this very significant risk.

Obtain a PDF version of this paper

Executive Summary

Third parties are an important part of most companies' business, products and services. ***Third-Party Risk Management*** (TPRM) attempts to manage the risk from integrating third-parties into a company's business. These risks can be service disruption, regulatory, political, more recently *Environmental, Social and Governance* (ESG) is a concern, as well as loss of intellectual property and data breach.

But current **TPRM** does not always consider ***cumulative*** third-party risk (henceforth cumulative-risk), the risk from the number of third parties that could impact the company in the same way, for example, from a large data breach. Because **TPRM** programs tend to evaluate vendors individually and because cumulative-risk is often many times greater than the risk from any single vendor, companies are left ignorant of a significant *operational* risk to the business.

Cumulative-risk can be managed as incident-frequency for a given impact type and severity. For example, a data breach affecting 100,000 people will happen every 5-years on average; a 1-hour loss of service will occur twice per year on average. Calculating cumulative-risk in this way risk allows a company to manage this risk to the business in the following ways:

1. **Understand** expected incident-frequency; track towards incident-frequency goals,
2. **Prepare** for incidents that are expected to occur more frequently,
3. **Avoid overreacting** when an expected incident does occur.

We propose a senior management ***committee*** to decide incident-frequency goals, while also considering the business consequences of meeting those goals. The stakeholders might include the **CFO**, the **Chief Risk Officer** (CRO**)**, **Quality,** the **Data Protection Officer (**DPO**)** and **Legal**. We explain how each might consider cumulative-risk and decide incident-frequency goals for their corresponding roles in the corporation, including regulatory, impact to customers and impact to the company.

We propose the **TPRM** team report to the **CRO**, to 1) elevate consideration of cumulative-risk, 2) avoid conflicts of interest and 3) support accuracy and objectivity when measuring cumulative-risk. TPRM might report elsewhere and we discuss the pros and cons of different purporting.

Risk is not accurate unless accumulated across all vendors, we therefore propose a single **TPRM** team that will work closely with **Procurement** to obtain and manage a complete vendor list. We also propose the **TPRM** team work with **Procurement** to leverage the vendor contract in order to compel needed remediation and future **due-diligence**. ***Avoidance*****,** a process of eliminating the impact, is the most effective way to measurably reduce cumulative-risk. We recommend **Procurement** consider the cost of **avoidance** when it is needed**,** but also the *value* that comes with lower-risk vendors, when negotiating contracts.

Finally, we recommend ways that the effectiveness of **due-diligence** can be improved: 1) by focusing on vendors that contribute most to cumulative-risk, and 2) by considering ***avoidance*** for vendors that contribute most to cumulative-risk.

With new tools to measure cumulative-risk, with incident-frequency goals set by senior management, we recommend that the **TPRM** team document standards for vendors that include when **avoidance** should be considered and how senior management can authorize the use of a vendor that prevent meeting the incident-frequency goals recommended by the **committee** and authorized by board.

Table of Contents

Introduction

Companies are evermore integrated with vendors (aka third parties). 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 risk management software, HR services and benefits, accounting, and customer relationship management (CRM). We have third-party services for monitoring fraud, providing transaction processing such as online banking, third-party services for marketing and lead generation, outsourced call-centers and third parties providing accounting services. While these third parties bring empowering technologies and significant cost savings they also bring risks from service disruptions, risks from data breach as well as regulatory and sanction risks. A small company can have 50 to several hundred integrated third-party partners; a large company can have literally thousands.

Third-Party Risk Management (TPRM) which consists of a framework and Third-Party Management lifecycle aims to establish appropriate governance to protect the organization from such risks. But TPRM programs are failing to measure the true nature of this risk—which is the **cumulative risk from the number of vendors**. It is important to understand that even when controls are implemented as part of due-diligence and remediation, the risk from each vendor is not zero. Even when the probability is very small, the probability of an incident increases with each vendor, and can become significant with a large number of vendors.

Most TPRM programs do not explicitly account for the cumulative-risk from the number of vendors and this risk is exacerbated if there is insufficient operational capacity to adequately assess all vendors while also monitoring critical vendors. We argue that insufficient operational capacity is the result of not quantifying cumulative-risk, leaving organizations unknowingly vulnerable. To take one kind of risk, data breach, we find that more than 50% of data breaches affecting 100-thousand or more people are caused by third parties. Yet the level of resources devoted to preventing third-party data breach is not commensurate with the risk exposure they present.

We will review the key components of current TPRM practice and show where current practices can be improved by including cumulative-risk, both making TPRM more efficient and helping the TPRM team better communicate third-party risk to the organization leadership. When cumulative third-party risk is quantified, it also allows consideration of a whole new set of strategies for reducing third-party risk, such as reducing the number of critical vendors through **avoidance**, or choosing multiple services from a single vendor instead of multiple vendors.

Following are some of the points we will address:

- Leveraging existing corporate structure to support quantifying, reporting and mitigating cumulative-risk.

- How cumulative-risk can best be reported.
- How to improve the efficiency of the TPRM vendor review; and how to reduce the burden to the business.

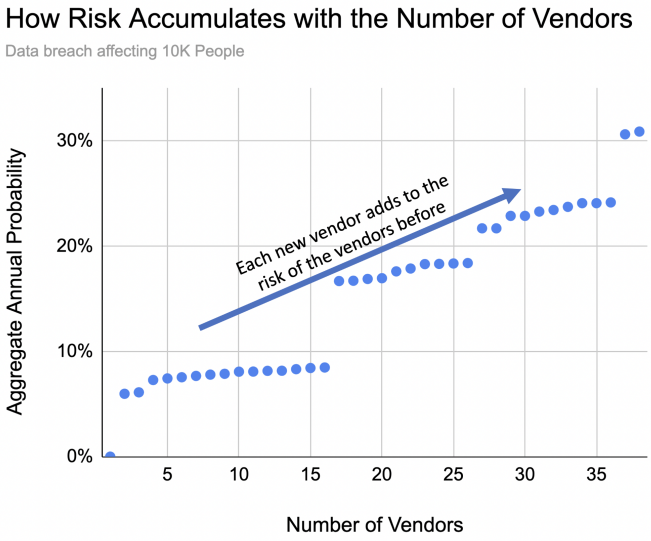
What is Cumulative-Risk?

We assume that the reader is familiar with the definition of risk, that risk is the cost of an incident[1] multiplied by its probability.

Cumulative-risk is the total risk that amounts from the existence of several simultaneous, but independent risk factors, here: multiple third-parties which each constitute an individual risk by themselves. In the case of data breach for example, cumulative-risk is the cost from exposing data multiplied by the sum of the probabilities for each third-party that could expose data.

Not all third-party risks are cumulative and some probabilities are reduced by more third-parties. For example, operational-resilience is improved and the likelihood of service disruptions is reduced when multiple third-parties can provide the same service. This white paper focuses on third-party incidents that do accumulate with the number of third-parties, such as the likelihood for a data breach. Also, financial institutions sometimes aggregate risk across incident types. In this white paper we are talking about accumulating risk across the same incident type and severity.

Many of the examples below will be **specifically for reportable PII data breach** through third-parties, since there are now models that accurately forecast probability for this incident type.



Let's look at the example of an organization that entrusts multiple vendors with its clients' and/or employees' (identifying) personal information and wants to know the probability that the organization suffers a data breach of e.g. 10K people's records. The graph to the right shows how the probability for a third-party

[1] The cost of an incident can be difficult to determine since companies are not compelled to report incident costs. *Environmental Social and Governance* (ESG) incidents have become a focus recently and the cost of these incidents are difficult to assess. One approach is to estimate the amount of marketing it would take to repair reputation or brand damage caused by these kinds of incidents. We also discuss the use of case studies below to help quantify the costs of such incidents. There are also peer reviewed papers on the cost of incidents, such as the impact of an incident on the company's stock value.

data breach increases with the number of vendors, for an actual company. Each dot in the graph is an actual vendor for the organization. The upward sloping curve was calculated by adding the probability for each vendor to the accumulated probability for the vendor to the left. The graph shows that as the number of vendors grows, the cumulative probability increases. The jumps are vendors that have significantly higher probability.

Cumulative probability is always much worse than the probability for any particular third-party. As an example, if a company has ten suppliers, each with a once in 100-year likelihood of exposing data in a data breach, then the cumulative probability for a third-party data breach is now once in 10-years.

We can also think of cumulative probability as rolling a die to obtain a particular number, e.g. a “one”. Each roll of the die has a one-in-six, or 16%, chance of obtaining a “one”. The chance of obtaining a “one” in multiple rolls of the die is simply the sum of 16% across all rolls of the die. We should obtain a “one” every six rolls of the die—on average. Or, when rolling six dice simultaneously, obtain a “one” on one of the dice each time – on average.

The concept of cumulative-risk is not new. Banks measure and manage this risk among a portfolio of loans; insurance companies measure and manage this risk among a portfolio of policies. It is common sense that a larger portfolio of loans will have more loan defaults; a larger portfolio of policies will have more claims; a larger set of vendors will have more incidents.

How to Think About Cumulative-Risk

Considering cumulative-risk in TPRM will bring surprises and new thinking. For example, traditional thinking is that because third-parties are an extension of your organization, you should expect the same level of security that you have for your own organization. But, with the once in 100-year example above, you can see that you should demand a much lower probability from your third-parties than from your own organization.

Current TPRM

The complexity and sophistication of current TPRM frameworks will vary depending on the industry, regulatory environment, maturity of the organization, management prioritization and ultimately the investment that is made available. But generally, the differences boil down to the breadth of risks considered.

Following is an overview of the key components of current TPRM programs:

1. **Pre-contract, analyze internally**, the impact-types and impact-severity[2] presented by each vendor, in order to assign a criticality level or tier,
2. **Pre-contract, vendor due-diligence**, using questionnaires, ratings and on-site visits, with the scope determined by criticality level,
3. **Pre-contract, avoidance or remediation**[3] based upon impact-types and findings from due-diligence, with remediations addressed in the contract.
4. **Post-contract reviews and remediation** with a frequency determined by criticality level and contract review,
5. **Continuous Monitoring and remediation** for critical vendors, using independent data such as adverse media and data breach intelligence.

There are several things to notice. First, the contract with the vendor is an important point of focus, since it provides the leverage to compel a third-party to take needed remediation actions, and it allows a decision not to use a third-party when a vendor exposes a company to too much risk. Second, vendors are ranked based upon impact—not probabilities. There may be an assumption that remediation drives the probability for an incident to zero—but it does not.

Structure of TPRM

Centralized vs Federated Program

The operating models adopted by an organization for TPRM vary with some organizations adopting a centralized model, others a federated model and some a combination of both models. We will discuss the reasons for different models and then discuss an approach that can incorporate cumulative-risk.

A federated model is convenient for dealing with local vendors in the case of multinational companies or companies with offices or divisions in different time zones. This is convenient since it is easier to negotiate contracts locally and compel needed changes before signing contracts (see reconciliation, below).

[2] Together impact-type and impact-severity are sometimes referred to as inherent risk which means the maximum possible impact if an incident did occur.
[3] **Remediation** is the process of addressing gaps that are discovered in control objectives, during the process of due-diligence. Often, control objectives are prescribed for certain impact-types, and these must be in place before the contract is signed. **Avoidance** is the process of eliminating the possibility that the vendor could impact the company, for example by blinding data that is shared.

In some organizations, TPRM is separated by impact-type[4] and accordingly assessed by different business units. Since - as explained below - third parties often present multiple impact-types, in this approach important cumulative-risks might be overlooked. An example is pharma and biotech industries which often divide third parties by GXP[5] and non-GXP. The GXP risk is managed by the **Quality Assurance** (QA) team. But these third parties might also present cybersecurity risks for example, which are overlooked when focusing solely on GXP risks.

We Recommend a Centralized Model

We recommend using a centralized model since quantifying risk from only a portion of third parties will underestimate the cumulative-risk.

It might seem strange to discuss the reporting structure for the TPRM team in this white paper, but we feel that it is important for objectivity, consideration of cumulative-risk and for the adoption of a common set of standards for evaluating third-parties.

We propose that the TPRM team report close to the **CEO** in the corporate hierarchy to foster appropriate consideration of the risk to the business. For example, the TPRM team might report to the **Chief Risk Officer** (CRO) for organizations that have a **CRO**. The **CRO** understands cumulative-risk and would have no conflict of interest in objectively assessing third-parties.

In the past, the TPRM team might have reported to the **CTO** or the **CIO**, because so much risk is data related. But financial regulators in the United States strongly recommended against this reporting structure since there was a conflict of interest objectively reporting on the risk from certain vendors that might bring desired technology to IT and the enterprise.

The Committee

We recommend a ***Committee*** to consider cumulative third-party risk. The stakeholders might include the **CRO**, the **CFO, Quality**, the **Data Protection Officer**[6] (DPO) and **Legal**. This group should 1) consider the current expected cumulative incident frequency, 2) opine on frequency goals that are right for regulators, the business and its customers, and 3) budgets that are needed to reach these goals.

[4] Some TPRM programs might call these risks. Again, we are careful to use the term risk when we mean ***Probability*** and ***Impact*** combined.
[5] GXP stands for Good *Manufacturing* Process, Good *Development* Process etc. where standards are specified by government regulators. Third parties involved with any of these processes, including companies that manufacture drugs, technology companies that hold the data, manuals etc. in databases or SaaS applications.
[6] For companies subject to GDPR

Why the CRO is Part of the Committee

We propose that the **CRO** be part of the **Committee** because their job is to accumulate risk across the company and present this risk to the board and senior management. In the case of cumulative third-party risk, the CRO would present the **Committee's** recommendations to the board, then convert the board-approved goals into policies for the corporation. Importantly, the **CRO** also has the education and training to evaluate model risk[7].

Why Quality is Part of the Committee

We propose that **Quality** be part of the **Committee** because they are responsible for setting the company standards and quality goals for the company's offerings. Third-parties are an integral part of the products and services for almost any company, whether they are a contract manufacturing site for a pharmaceutical company, or an IaaS third-party hosting a database that is an important component of a SaaS offering. In a Pharma and Biotech, **Quality** would consider the patient first. In the case of all other industries they would consider the customer first.

Quality's goals are most often expressed and managed as incident or defect rates, so setting and managing target third-party incident rates naturally fits into **Quality's** existing defect or incident rates management framework and lifecycle.

For companies that view quality of their products and services as a competitive advantage, **Quality** has the experience working with senior management, the **CFO** and the **CEO** to weigh the cost of achieving quality goals, and in the case of Pharma and Biotech, **Quality** even has the power to disqualify a third-party.

Why Legal is Part of the Committee

We propose that **Legal** be part of the **Committee** because much of third-party risk is regulatory related, such as protecting various kinds of PII, and the **Legal** departments are concerned with ensuring that the company is meeting regulations and the law. In the following section we suggest ways that **Legal** might consider expected frequency of third-party incidents, that fulfills their traditional role of ensuring that the company follows the law.

We also feel that the contract with the third-party is very important for managing cumulative-risk and **Legal** can support the drafting of enforceable contracts that can manage this significant risk.

[7] Model Risk is a term used to describe the risk from making business decisions using a model that forecasts an incident. For U.S. banks, management of model risk is covered by The Federal Reserve and Office of the Comptroller of the Currency supervisory guidance, SR 11-7.

Why the DPO is Part of the Committee

A **DPO** is mandatory under GDPR, and should be part of the **Committee** for organizations that fall under any regulatory obligation for data protection. One of the **DPO's** obligations (according to GDPR Art. 39) is "to provide advice where requested as regards the data protection impact assessment and monitor its performance" whereas a data protection impact assessment needs to be performed (according to GDPR Art. 35) "where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons", the latter ("high risk to...") being the central theme in GDPR.

The **DPO** is similar to **Quality** in the Pharmaceutical, Biotechnology and other industries in that they regard people before the corporation.

Why the CFO is Part of the Committee

We propose that the **CFO** be part of the **Committee** because, now that third-party risk is quantified in real money terms, it becomes a financial issue. Goals will most likely be met by the process of **avoidance** (see below) which will cost money and effort. The accuracy of cumulative assessments will also be a function of the resources that can be spent on the TPRM team itself. It is more efficient to have the **CFO** as part of the **Committee** to help decide cumulative-risk goals that can be achieved with the financial resources available, and how the company will prepare for expected third-party impacts. In some companies, it will be the **CFO** that brings possible third-party risk plans to the board for a decision.

Presenting Cumulative-Risk

The **Committee** will consider cumulative-risk, decide risk goals and budgets to meet those goals. The challenge is to present this cumulative-risk in a credible and useful manner. We will address credibility at the end of this section. First, we will address the most useful ways of presenting cumulative-risk.

We propose that cumulative-risk be presented to the **Committee** as cumulative-probabilities calculated for various levels of impact severity. For example, cumulative-probability for data breach would be calculated for a data breach affecting 10K people, 100K people, 1M people etc..

Furthermore, we recommend that probabilities reflect cumulative-probability for an incident occurring within the set of vendors. For example, the cumulative-probability for a data breach would simply reflect frequency of a data breach among the vendors, where the data breach may or may not include your organization's data[8]. The reason for this simplification is that it is hard to generate rigorous statistical

[8] Each vendor's probability could be further adjusted to include an estimation for the probability that the beach would expose your company's data. For example, if a very large vendor had a very small data breach, it would be unlikely to include your data. We suggest that this estimation be part of due-diligence activity.

models that would forecast incidents that would impact your organization, while it is easier to generate models that forecast an incident generally.

The table demonstrates how we recommend presenting cumulative-risk for a third-party data breach. The table shows the probability for a data breach happening among 38 vendors that could expose some kind of PII[9] data, broken down by six data breach sizes. For example, the table shows that there is a once in 7-year probability that one of the vendors will have a data breach affecting 10K people.

Breach Size (People Affected)	Aggregate Annual Breach Probability Aggregate Breach Frequency	
	Industry Median (σ)	Company (38 vendors)
1000	29-years (45) 3.5% (2%)	11-years 9.1%
10,000	63-years (85) 1.6% (1%)	7-years 13.4%
100,000	13-years (10) 8% (10%)	10-years 10%
1,000,000	43-years (42) 2% (2%)	27-years 3.8%
10,000,000	374-years (324) 0.3% (0.3%)	238-years 0.42%
100,000,000	2,356-years (2,273) 0.04% (0.04%)	1326-years 0.1%

Presenting Cumulative-Risk to Legal or the DPO

We feel that for **Legal** or the **DPO**, the best way to consider cumulative-frequency is by comparing it to an industry median. Most regulations and standards expect companies to measure risk ***accurately***, which requires measuring cumulative-risk since this is the major risk from third parties, and to take ***reasonable*** steps to mitigate risk.

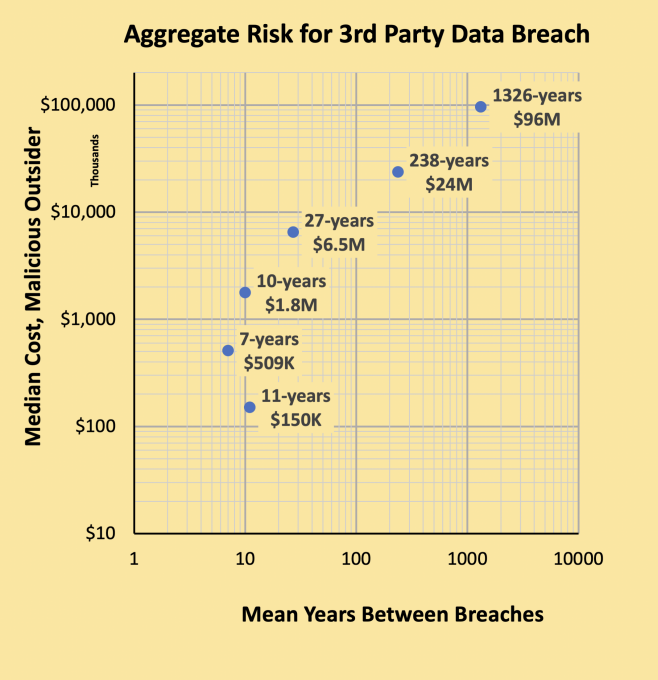
For example, in the United States, HIPAA regulation 45 CFR 164.308 (a)(1)(ii)(A) requires "...**accurate** and thorough..." and 45 CFR 164.308 (a)(1)(ii)(B) requires "...**reasonable** and appropriate…". To support an argument for reasonable and appropriate, the table also shows an industry median for each breach size. For a data breach size of 10,000 people affected, **Legal** would be able to argue that a breach frequency of once in 7-years is significantly worse than the industry median of 63-years and therefore not "reasonable and appropriate". We realize that *reasonable* tends to be determined on the basis of whether the precautions taken were consistent with industry standards rather than assessed on the basis of whether an *ex ante probability* was within industry range[10]. However **Legal** now has new information with cumulative-risk calculated and we propose that they advise the company on the basis of what is ***necessary*** rather than simply what is ***sufficient*** regarding protecting various kinds of PII data.

Presenting Cumulative-Risk to the CFO

Besides helping to decide budgets to meet cumulative-frequency goals, the **CFO** might also decide to set aside reserves to cover the costs of a third-party incident. This is a common approach for anticipating future losses, similar to setting aside funds for product warranty by companies that manufacture

[9] PII is nonpublic Personal Identifiable Information, such as a person's name and their driver's license number.
[10] The reason the *ex ante probability* is not adopted is that probabilities are usually hard to verify, even with expert testimony, while industry standards for precautions are relatively easy to verify.

hardware, for 'shrinkage' (theft and spillage) in super markets, or for fraud in financial institutions. If costs can be calculated, then presenting cumulative-risk as shown below in a risk matrix would allow the **CFO** to understand both the cost and frequency and decide what should be set aside. However, we understand that a **CFO** might also prefer to spend the money to reduce the cumulative-frequency since Sarbanes Oxley auditors don't like setting aside reserves, considering these to be slush funds.



The matrix shows the frequency data from the table above and combines this with the median costs for data breach caused by a malicious outsider attack. Costs were calculated using a regression analysis of 100 data breaches with known costs. The matrix shows, for example, that a data breach with a median cost of $500K is expected to occur every 7-years on average, and a $1.8M data breach every 10-years on average across 38 vendors. The **CFO** can set aside funds to cover the cost for the near-term events. These funds would count against profits and this would get the attention of the board of directors. The board can recommend increased funding for TPRM to decrease the size of funds that are set aside by the **CFO**.

In the matrix to the right, we have used a regression model for the total cost of a data breach. Another approach to estimate cost is using incident scenarios[11]. Scenarios can also be used to refine the costs from a regression model. For example, the regression model we used had a large 80% confidence interval and scenario analysis could be used to see how costs might be reduced, justifying the use of the median cost rather than the 80% confidence interval.

Managing Risk Well is a Competitive Advantage

Once the incident frequency is understood and the next incident can be anticipated, the **Committee** can set goals for the company and recommend an increase in TPRM funding to reach these goals. Some would say it is a competitive advantage for a business to efficiently manage risk. Efficiently managing risk means understanding incident frequency and taking sufficient measures to protect the organization from the expected financial impact; not overreacting when the expected incident does occur; not overspending to mitigate rare events.

[11] O.R.X. (ORX.org) for financial institutions, also *Cyber Security Case Studies* (cybersecuritycasestudies.com).

Meet Goals with Avoidance

For data breach risk, the main tool for reducing cumulative-risk is **avoidance**. **Avoidance** reduces risk by eliminating the impact. Examples of **avoidance** are 1) blinding data that might be shared with a vendor, 2) encrypting data within a database on a vendor's server so that even if there was a network intrusion the data could not be accessed, 3) having an internal policy not to put sensitive data within a vendor's application, such as Google Apps or SalesForce.

Remediation activities may reduce probability of an incident, but unless one has a statistical model that specifically includes the remediation as an explanatory variable[12] or unless the remediation leads to a change in an explanatory variable, the reduction in probability generally cannot be quantified.

We discuss **avoidance** more below.

Model Risk

The **Committee** should also consider model risk, which is the risk from making a business decision based upon the model. Models must be credible if management is to make business decisions based upon the models. The United States Federal Reserves has put out a standard for model risk management called SR 11-7 which can be used to assess model risk. Larger financial institutions have a model validation team that is able to review a model per SR 11-7.

For data breach models, a simple way to evaluate a model is to compare a future forecast to the history of data breaches. Generally future forecasts match the history of data breaches, over a large set of vendors.

Working with Procurement

We recommend that the TPRM team work closely with **Procurement** (aka Purchasing) to achieve a centralized model. We propose **Procurement** as a TPRM partner because they already deal with all vendors for the company (any vendor that wants to get paid[13]) and can therefore ensure a complete list of third-parties.

Another reason for the TPRM team to work closely with **Procurement** is because the procurement department tends to include lawyers who are good at negotiating contracts, and the vendor contract is a powerful tool to compel needed remediations.

Another reason for the TPRM team partnering with **Procurement** is that their goals are often aligned with saving money for the organization and vendors bring more than the value of their services. Some also bring more risk; while others bring more robust security, more financial viability, more operational

[12] In an empirical regression model, *explanatory* variables are the variables used to predict.
[13] It is not uncommon for a company to work with a vendor to perform a proof of concept (POC) or trial. Ideally there should still be a contract in place and involvement of procurement, since the vendor is performing the POC with the hope that it will eventually lead to a paid contract.

resilience, and some bring more products and services, which reduces cumulative-risk by reducing the number of vendors[14]. When each vendor's contribution to cumulative-risk is calculated, this additional value, or cost, can be leveraged during contract negotiations. As we show below, a single vendor can double the probability for a costly data breach for example, and result in the extra cost of **Avoidance** (explained below), or the **CFO** setting aside funds to cover this increase in risk, or purchasing insurance to transfer the risk. It can cause the cumulative-frequency to exceed a level that **Legal** or the **DTO** deem reasonable as explained above. In other words, saving money and reducing costs associated with cumulative-risk can go hand-in-hand, and both can fit within the traditional goals for **Procurement**[15].

Delivering a Schedule of reviews

The implementation of a TPRM framework can be complex and time consuming. Below we outline the effort for each vendor, and we show where efficiency can be improved by considering cumulative-risk.

If there is a large population of third-party suppliers already in use, those suppliers will need to go through an initial due diligence process to act as a baseline risk assessment. This can sometimes be confusing for those existing suppliers who have not been asked previously to complete questionnaires, or demonstrate good governance processes. If issues and exceptions are identified but contracts are already in place, the support of business owners and procurement teams becomes vitally important to manage the new expectations. Internal stakeholder management and communication is critical to the success of any TPRM framework.

Conducting due diligence on new potential suppliers can be less confusing for vendors as they will not have become familiar with any other process. However, initial due diligence can be more time critical if contract negotiations are taking place in parallel. Typically, a team responsible for implementing and embedding TPRM will have to manage a pipeline of work comprising of:

- ***Planned reviews*** of known existing suppliers,
- ***Unplanned reviews*** of new suppliers, the timing of which is dependent on whether and when the business decides to request products or services from these supplier(s).

In subsequent years the pipeline and schedule of reviews will grow to include ongoing monitoring assessments.

[14] For example, in the case of data breach, the probability increases as the sum of probabilities across each vendor that can expose data. Using a single vendor that supplies multiple services rather than multiple vendors to supply multiple services, therefore lowers the probability for data breach.
[15] One of the authors has seen TPRM reporting to **Procurement** in several large financial institutions—with great success. These organizations did have a well rounded **CPO** who understood third-party risk concerns.

The Resource Challenge

The challenge for many organizations is managing and prioritizing limited resources to deliver a schedule of reviews. Invariably there are not enough resources available to complete assessments on all the suppliers and risk-based decisions need to be made in relation to what does not get done. In some cases the sequencing of assessments is driven by a time constraint such as contract dates.

For example, let us assume that reviews of new potential suppliers have to be conducted as and when requests to procure new products or services from new suppliers are received. These will be considered unplanned reviews as there is limited control over the number and cadence of such reviews.

Let us also assume that an existing population of third-party suppliers has been segmented (or Tiered) into High, Medium and Low impact suppliers. Typically an organization should aim to assess the riskier suppliers first (i.e. High and Medium). The timing of each review may be dictated by a logical event or intervention such as a contract renewal date, anniversary of the contract start date, etc. Using a contract renewal date for instance, may help motivate a supplier to provide more timely due-diligence information when requested.

The result of this scheduling exercise will be a plan of reviews that need to be conducted throughout the year. At the highest level TPRM teams may be expected to provide management reporting on amongst other things:

- Successful delivery of the review plan i.e. planned vs completed,
- Coverage of assessments over the supplier population i.e. how many suppliers have been reviewed,
- Assessment results,
- Assessment efficiency i.e. how many days did it take to review a supplier
- Issues identified, etc.

The achievement of the first two measures is dependent on the availability of resources to deliver. However, when operationalizing a TPRM framework it can be easy to overlook a key tenant—the need to reduce risk. While the High, Medium and Low tiers are a representation of relative risk, it may be that suppliers can be further differentiated through an enhanced triage approach using probability models.

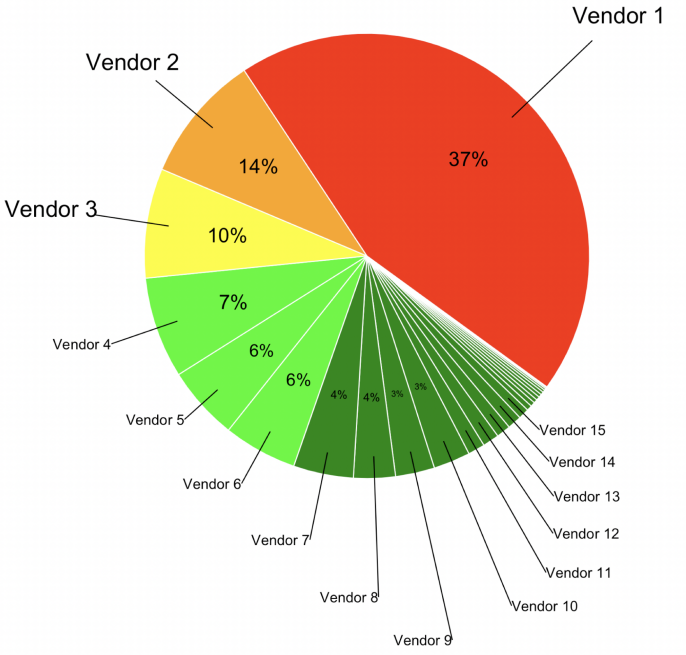
Use of Probabilities to Address the Resource Problem

To help prioritize review and simplify vendor due-diligence, we propose using any accurate models available for probability of the relevant incidents.

Unlike ***scores***, ***probabilities*** directly relate to the likelihood of an impactful incident. That's what they are: the likelihood that an incident will occur.

Accurate models tend to find large differences between companies. For example, some companies will have a very low probability, e.g. once in 1-thousand, other companies will have a high probability, e.g. once in five.

As an example, recent *Probability Models for PII Data Breach*[16] could be used to simplify due-diligence for vendors that present mainly data breach risk. The end goal of due-diligence is to reduce the probability for a data breach and the most efficient way of reducing probability is to focus on the vendors that represent the largest proportion of cumulative-risk. Since accurate models for the probability of an incident tend to find orders of magnitude differences between vendors, often just one or two vendors will represent 50% or more of the cumulative-risk and these are the vendors that should be focused on first.



The pie-chart shows the breakdown for the probability of a data breach affecting 10K people across the company's 38 vendors that have the potential to expose data. Each vendor's proportion of cumulative-risk was calculated by dividing the vendor's probability by the cumulative-probability (the sum of probabilities across all vendors). Vendor names are not shown since this represents a point in time and vendors may have changed since this analysis.

Vendor-1 and Vendor-2 together represent 51% of cumulative-risk (14% + 37% = 51%). Eliminating the risk from just these two vendors, for example through **avoidance**, would reduce cumulative-risk by half (i.e. double the mean years between incidents). For this example, the frequency for a data breach affecting 10K people would improve from once in 10-years to once in 20-years. On the other hand, mitigating risk from vendor-10 which represents 3% of the cumulative-risk would make little difference in reducing the overall probability of an incident.

Focusing due-diligence on vendors that contribute most to cumulative-risk will also reduce the impact to the business. Due-diligence reviews and data collection can take weeks, delaying the onboarding of new vendors which delays any value these new vendors might bring to your organization.

[16] Models for the probability of any kind of PII data breach are available from VivoSecurity.

Remediation & Avoidance

Current TPRM relies upon **remediation** to reduce the probability of an incident. **Remediation** is the process of having a third-party address issues which were discovered during due-diligence. These issues might be gaps in control objectives, for example. A control objective might be a TPRM program, or two factor authentication for emails accessed externally.

Avoidance on the other hand eliminates the likelihood of an incident by eliminating the impact. In the case of a data breach, an example of **avoidance** might be blinding data that is shared with a third-party. Another example might be the encryption of a database that resides within a third-party, like Amazon Web Services (AWS).

Current TPRM can be greatly improved by also including **avoidance**, once cumulative-risk is measured. We will explain **remediation** and **avoidance** in more detail below.

Measuring Cumulative-Risk Justifies Avoidance

Since the statistical probability for a data breach is a cumulative probability, reducing the number of third-parties reduces cumulative-probability. But without an accurate model to identify each third-party's contribution to the cumulative-risk, **avoidance** is not worthwhile on an individual vendor basis.

In the pie chart above, most of the 38 vendors are not worth **avoidance**—individually. For example, Vendor-10 represents only 3% of the cumulative-risk and **avoidance** for this vendor would not make a significant reduction in risk.

Avoidance	**Frequency** (years)
None	10
Vendor-1	16
Vendor-2	12
Any single Vendor-3 through 5	11
Any single Vendor-3 through 5	11
Any single Vendor-6 through 38	10

The table to the right demonstrates this, by showing how the expected cumulative data breach frequency would change if any single vendor were mitigated. The table shows that **avoidance** for any single Vendor-6 through Vendor-38 would leave the forecast frequency essentially unchanged.

With an accurate model however, the vendors worth the effort to apply **avoidance** can be identified, and **avoidance** can now become the most effective way to reduce cumulative-risk. For example, the table shows that applying **avoidance** to vendor-1 would improve the cumulative-frequency from once in 10-years to once in 16-years.

Of course it is a good policy to reduce the number of third-parties that could impact your company, even without a model. With the vendors presented in the pie chart, about one in ten vendors have a high

probability, and even when vendors have a low probability individually, the cumulative-risk across a large number of vendors with individually low probability, does become significant.

Remediation

Remediation often addresses gaps in control objectives that were discovered during due-diligence. The best time for remediation is during contract negotiations; remediations should be written into contracts and ideally addressed before contracts are signed. Contracts should also include provisions for future remediations when post-contract periodic due-diligence is performed.

Goals, Policies and Methods

If the **Committee** sets goals, it makes sense for the TPRM team to draft policies and methods that should be followed to reach and maintain those goals. These policies and methods would not be only from the perspective of control objectives, but also from the perspective of a vendor's contribution to cumulative-risk. They could specify when **avoidance** should be pursued, when a waiver from senior management would be needed to bring on a vendor that would constitute a large portion of cumulative-risk or would cause cumulative-risk goals not to be met. These policies and methods could guide how vendors might be chosen. For example, using a single vendor that offers multiple services, instead of receiving the same services across multiple vendors, can reduce the burden for the TPRM team and also reduce incident frequency.

The Contract

We would like to conclude with the contract, which is the focal-point-in-time of TPRM. For cybersecurity, the vendor contract might be the key to improving security in general.

The contract is the mechanism by which a third-party can be compelled to perform needed actions to reduce your third-party risk. In current TPRM, the contract should address the following:

- Remediation and verification
- Periodic access for due diligence
- Future remediations
- Possible involvement of another company to help with due-diligence

Address the Underlying Cause

When considering cumulative third-party data breach risk, we have a bold proposal: address the underlying cause.

When due-diligence reveals gaps in control objectives, think about why the gaps are there. Why did the vendor fail to recognize an important risk? Empirical regression models suggest that it is because the vendor has an insufficient number of cybersecurity and audit/compliance employees to recommend, deploy and monitor the controls, and also enforce compliance. Addressing gaps in controls is important but the underlying cause still has not been addressed.

When the vendor accounts for a significant portion of the cumulative third-party risk, we propose asking the vendor to increase the cybersecurity headcount as well as audit and compliance headcount. The argument can be compelling when a vendor is shown how much they will increase your cumulative-risk based on an accurate empirical regression model. It can be especially compelling when the vendor is compared with their competitors. Often the comparison is dramatic with the competitor having two or three times the number of cybersecurity, audit and compliance employees. Contract negotiations are a time when a vendor can be made to understand that investing in security is good business and a competitive advantage that can increase sales.

Conclusion and a Science Based Approach

We have shown how cumulative-risk is the major risk from third-parties, we have proposed a reporting structure to facilitate accurately measuring and reporting this risk, we have suggested several ways cumulative-risk can be considered and reported, we propose a **Committee** to opine on frequency goals and we have shown how goals can be met through **avoidance**.

Regarding data breach risk, TPRM teams can begin right away to apply the tools to prioritize vendors for due-diligence. Usually just a few vendors are responsible for most of the cumulative data breach risk and these vendors should be the main focus. ***Avoidance*** can reduce the burden of due-diligence, simply by reducing the number of vendors that need to be considered[17], but until management sets cumulative frequency goals, it is hard to justify the cost of implementing **avoidance** strategies.

Finally, we would like to point out that the number of data breaches only increases year-by-year, and when we collect data on companies the reason is clear, many companies simply have not invested enough in cybersecurity, have not hired enough cybersecurity employees, and have not hired enough audit/compliance employees. This increase in data breaches is despite increasing regulation and privacy laws, and despite more cybersecurity controls.

We propose that the TPRM portion of vendor contracts, along with a science based approach for measuring third-party data breach risk, could promote one of the most important improvements to

[17] Note that even with **Avoidance**, the TPRM team would still need to periodically investigate internally, that impact has been eliminated.

cybersecurity. Contract negotiations are the best time to show vendors the risk that they present, the best time to convince vendors that an investment in security is a competitive advantage. Perhaps TPRM, with the right tools[18], can do something that regulation and privacy laws could not—promote better security.

[18] Please contact the authors to learn about these *Empirical Regression Models for PII Data Breach*.

Appendix

Glossary

Avoidance	Actions taken to remove the risk, by eliminating the impact. An example might be encrypting a database that resides in AWS. Even if AWS is breached, the data cannot be accessed.
Criticality or tier	Ranking or grouping of vendors based upon their potential impact.
Cumulative-Frequency	The expected frequency across all third-parties for a particular incident type and impact severity.
Cumulative-Risk	The risk across vendors for a specific risk type and impact severity. Risk from the number of vendors.
Impact	The financial impact to the organization if an incident occured
Impact-severity	The financial impact for a particular incident-type.
Incident-types	A specific risk type, for example, financial risk.
Model Risk	The risk posed by making a business decision based upon a model. This risk is a function of the model accuracy. The United States Federal Reserve System and Board of Governors provides guidance SR 11-7 on Model Risk Management.
Operational Resilience	Result of organizational and technical measures to allow an organization continue its mission despite of incidents that negatively impact its operations
PII	Non-public, Personal Identifiable Information that triggers state or federal reporting requirements. Can include CHD (Card Holder Data), PHI (Protected Health Information), PFI (Protected Financial Information).
Probability	Probability for an incident, usually expressed as a percentage per year. Remediation Steps taken as a result of due-diligence of a vendor to address a gap to the organization's target level. Remediation does not mean that the risk is eliminated.
Risk	Financial impact of an incident multiplied by its probability
Vendor Due-Diligence	The process of reviewing vendors

Acknowledgements

We would like to thank the following people for their contributions to writing this paper.

Axel Troike

For providing feedback on how to explain cumulative-risk, terminology used in cybersecurity, corporate reporting structure and roles that should be part of the **Committee**, the role of the **GC** and **Legal** in interpreting cumulative-risk and a significant amount of editing. Axel Troike provides consulting services at the intersection of compliance, business and IT. With over 20 years of management experience, he has conducted more than 100 projects in 8 countries with focus on 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.

In current mandates, Axel conducts assessments on 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 guidelines for IT audits, performing audits of the software development process and implementing measures to mitigate identified risks and weaknesses. Axel helped a group of insurance companies during their restructuration (merger of business units and outsourcing of IT services) and was the project manager in developing a common claims application system in the post-merger phase. He holds a Master's Degree in Mathematics from Christian-Albrechts-University in Kiel, Germany. Axel can be contacted at `axel.troike@grandite.com` or via Linkedin.

Shawn Wilde

For providing feedback and insights into the role of the CFO and how risk should be communicated to the board, into the activities of vendor due-diligence and into the various legal requirements for companies that have PHI.

Until recently Shawn was the IT Director of Strategic Programs at Natera, a genetic testing and diagnostics company located in San Carlos, CA. He specialized in IT technical compliance for HIPAA, GDPR and the CCPA and provided IT management support for all lab operations compliance audits: CAP/CLIA, GMP, and NIST CSF. Prior to joining Natera Shawn consulted at various high tech manufacturers and until 2013 he was the Chief Information Officer at Trimble Navigation. While at Trimble he managed the IT systems and staff integration of over 70 acquisitions and joint ventures and managed the coordination of 10 federated IT organizations. Shawn is a board member of VivoSecurity and a lecturer at San Jose State University. Shawn can be reached at `shawn.wilde@gmail.com` and LinkedIn.

Paul Steiner, PhD, CQA

For providing feedback and insights into the role of QA in a TPRM program. Paul has a consulting business providing services in the areas of pharmaceuticals (GMP, GCP, GLP, GPVP) and medical devices with emphasis on quality systems, regulatory compliance, supplier qualification audits, chemical, manufacturing and control (CMC) and materials and process science (Advanced fiber composites and adhesives). Often serving as an expert witness in his consulting roles, he is also an ASQ CQA (certified quality auditor). He has performed over 200-300 audits spread over four continents in his career to date, primarily as lead auditor.

Before going into business for himself, Paul A. Steiner was the Head of Quality at the last few pharmaceutical companies for which he worked. He has worked in quality assurance (QA) in pharmaceutical / biopharmaceutical and medical device companies some of which included, Gilead, FibroGen, NGM Biopharmaceuticals, Vivus, and Affymetrix (recently acquired by Thermo Fisher) to name a few. With a Ph.D. in organic chemistry from the University of Washington and an undergraduate degree in chemistry and chemical engineering from Cornell University, he started his career at Bio-Rad Laboratories as a scientist working in R&D and process development/engineering. With roles of increasing responsibility in technical management, he spent most of his career working for companies which were to some degree “virtual” managing third-party contractors. Dr. Steiner has technical and management experience spanning all phases of the product lifecycle from early research and development through cGMP quality operations. Paul Steiner can be reached at `pasteiner11411@gmail.com` and LinkedIn.

Aaron Arutunian

For providing feedback on how risk can be presented to senior management and helping with TPRM as specified by various standards such as ISO 27001 and PCI DSS. Aaron is a senior consultant helping organizations to establish and optimize their information security and privacy programs, meet and manage their compliance objectives, and quantify their cyber risk. Aaron has more than 25 years of experience and 40 industry certifications, and his expertise encompasses a wide range of information technology, security, and compliance frameworks and standards. Aaron can be contacted at `aaron@grcallies.com` or via Linkedin.

About the Authors

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

Thomas is the CEO of the Silicon Valley based **VivoSecurity**, a company focused on data collection, regression modeling and AI to quantify cyber security risk. Thomas has spoken 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, multiple patents for quantifying cyber security risk. Thomas holds degrees in Physics and Electrical Engineering from the University of Washington in Seattle, and an MS and PhD in Biophysics from the University of Chicago. Thomas can be contacted at ThomasL@VivoSecurity.com and Linkedin.