An Enhanced Approach to Vendor Due-Diligence

David Hann
DHann Consulting
David@DHannConsulting.com

Thomas Lee, PhD
VivoSecurity
ThomasL@VivoSecurity.com

Table of Contents

Background

In this white paper we describe, step-by-step, an additional kind of vendor due-diligence for third party data breach, which significantly enhances the current practice of reviewing cybersecurity controls.

This new supplementary approach focuses on company size and staffing levels of people with specific certifications which have been found – empirically, to predict data breach with high accuracy.

Before we explain how to perform the due-diligence, we first explain the advantages of combining approaches.

Why attention to a vendor's staffing levels can reduce periodic review of Tier-1 vendors

In the current approach to **Third Party Risk Management** (TPRM), Tier-1 vendors are periodically reviewed using the traditional approach for vendor due-diligence. This frequency of review can be reduced by combining due-diligence approaches. You can understand why by comparing the combined approaches to the best practice for defect resolution: **Corrective** and **Preventive Action** (CAPA).

The focus of **CAPA** is not simply to correct a defect, but to also address the root cause. In **CAPA**, for example tightening a loose screw is the **corrective action**; addressing why the screw is loose is the **preventative action**. It is the **preventative action** that reduces future defects.

The traditional approach to vendor due-diligence for data breach risk, is based upon an examination of the vendor's cybersecurity controls. Gaps in controls that are considered important and are then addressed in the vendor contract through a process referred to as **remediation**. We discussed this approach in a previous white paper[1].

If gaps in cybersecurity controls are the defects, and the **remediation** process is the **corrective action**, what would be the root cause and what can the TPRM team use as the **preventative action**?

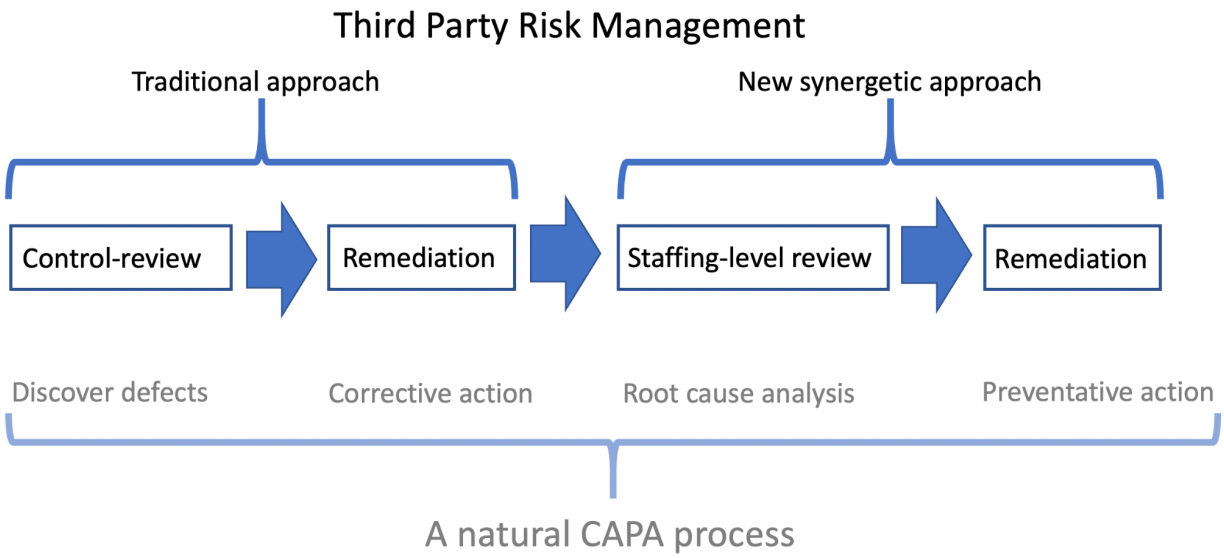
It turns out, inadequate staffing levels is the root cause.

We know that inadequate staffing levels serves as a root cause for any control-gap that is effective at preventing data breach, because regression modeling finds that the probability for a data breach can be accurately calculated based upon 1) company size, and 2) the number of certified audit/compliance and cybersecurity personnel that support a company. If addressing a control-gap is indeed effective in preventing data breach, then statistics tells us that the gap would have been corrected if the vendor had sufficient staffing levels.

The due-diligence we describe below therefore serves as a science based root cause analysis and the remediation based upon this analysis as the **preventative action** for any control-gaps

[1] How to Improve Third-Party Risk Management using Statistical Models, D. Hann & T. Lee

that are actually effective at reducing data breach. Implementing the **preventative action** should therefore reduce expected gaps in cybersecurity controls in the future and so reduce the need for Tier-1 vendor reviews.



The reason for framing these two forms of vendor due-diligence within the **CAPA** process is simply to help you understand the synergies between the two approaches. They need not be executed in the CAPA sequence, indeed the staffing-level analysis might be performed first so that the results can guide the depth of review for the traditional control-based approach. Staffing-level review might also reveal that the risk in using a vendor is too high and impact-reduction is the only option, thus eliminating the need for control-review.

Be compliant by quantifying cumulative third party risk

As we explained in a previous white paper[2], the probability for a third party data breach is a **cumulative-probability** – it is from the number of vendors that can expose your data.

Cumulative-probability can be calculated by simply summing the probabilities of the individual vendors. Due-diligence based upon qualified staffing levels has the additional advantage that it can be used to accurately calculate probability for data breach for each vendor and therefore accurately calculate **cumulative-probability**.

You can understand that **cumulative-probability** is the greatest risk, since it is simply the sum of the probabilities for each vendor that can expose your data, and therefore it must be larger than the probability for the worst vendor.

The current approach for vendor due-diligence and TPRM does not consider the number of vendors and therefore does not directly address the largest risk for third party data breach.

[2] How to Improve Third-Party Risk Management using Statistical Models, D. Hann & T. Lee

Since most regulations require addressing at least the largest risks, failing to directly manage the risk from the number of vendors means a company is non-compliant with most regulations for TPRM.

Why quantification can enable more outsourcing

Data breach risk is shifting due to increased outsourcing and third party data breach risk is rapidly becoming the major data breach risk for many companies.

Outsourcing can be good since third parties bring tremendous value: new technologies, new efficiencies, allowing a company to run lean and stay focused. But the current approach may limit the amount of outsourcing since management might be overly cautious with a risk they cannot measure.

The due-diligence described below includes methods for quantifying and strategies for managing the frequency of third party data breach as new vendors are added. These methods and strategies can give management the confidence they need to use more outsourcing and bring more efficiency to your company.

A better measure of TPRM effectiveness

Many TPRM teams are appraised based on the completion of a predefined assurance plan, for example reviews of all Tier-1 vendors. This infers – but does not quantify, a reduction of vendor risk.

Following the methodology in this white paper, the TPRM team's performance can be evaluated from a more quantifiable perspective: Reduction in **cumulative-probability** for a data breach. We will explain how to perform these calculations, and also give examples below.

The On-Demand Single Vendor Report

The staffing level due-diligence described in this white paper is designed around an ***On-Demand Single Vendor Report*** (On-Demand Report) produced by VivoSecurity. An example of this report can be found in the Appendix.

It is assumed that all of your vendors that could expose PII data have already been analyzed by VivoSecurity using the empirical regression model. VivoSecurity will therefore already know the **cumulative-probability** of your current vendors[3].

Report generation is often a two step process. In the first step, submit the name of the vendor to be analyzed. VivoSecurity will obtain headcount information without the assistance of the vendor and generate a report that will show:

- The current predictive headcount information for the vendor,
- Probability for PII data breach broken down by data breach size,

[3] Contact VivoSecurity for a cumulative risk assessment.

- Change in headcounts and probabilities if VivoSecurity has assessed the vendor before,
- Peer comparisons with companies in the same industry and same company size,
- The increase in **cumulative-probability** by data breach size that would occur if the vendor were on-boarded.
- The reduction in cumulative-risk by the TPRM team resulting from exposure-reduction.

In the second step, submit to VivoSecurity any changes you have learned or remediation you are requiring based upon your due-diligence. VivoSecurity will then regenerate the report with the new information and also show the value of your remediation activities. Examples are shown below.

Roles to carry out staffing level due-diligence

In our previous white paper[4], we recommend a management committee to decide **cumulative-risk**[5] goals that are right for the company. To reach these goals, new strategies will be followed that will require more than the technical role. These strategies include: requiring an increase in on-going cybersecurity consulting hours, requiring an increase in staffing levels, requiring an increase in training and certifications, dropping vendors, switching vendors, exposure-reduction and consolidating services. We see three roles in performing vendor due-diligence and remediation to achieve **cumulative-risk** goals:

1. **TPRM cybersecurity expert (operational):** judging the qualifications of the vendor's certified and non-certified cybersecurity personnel and consultants; recommending changes to headcount or consulting hours,
2. **TPRM team manager (tactical):** prioritizing on-going and initial vendor due-diligence; deciding the most effective way to reach cumulative-risk goals; advising the committee on achievable goals, approaching the committee when goals cannot be met,
3. **TPRM Committee (strategic):** setting cumulative-risk goals ahead of time, approving adjustments to cumulative-risk goals when it will benefit the organization.

For process efficiency, it is important that **cumulative-risk goals be determined beforehand**. This allows the **TPRM team manager** to decide how to meet these goals and it allows the due-diligence for each vendor to proceed quickly, when **cumulative-risk** goals are not put at risk. The TPRM team should therefore rarely approach the committee for the approval of a vendor.

The process of deciding **cumulative-risk** goals is a process of weighing the cost of meeting low **cumulative-risk** goals against the impact of 3rd party data breaches and is described in our previous white paper.

[4] How to Improve Third-Party Risk Management using Statistical Models, D. Hann & T. Lee
[5] Since probability is a strong function of data breach size, we often refer to cumulative-risk as the consideration of cumulative-probability as a function of data breach.

How due-diligence is organized in this white paper

This white paper only addresses staffing level due-diligence, but it is assumed this approach will be used in combination with traditional cybersecurity control based due-diligence.

Empirical regression modeling finds that company size is a major predictor of data breach. This is also in line with general thinking among cybersecurity experts, since the attack-surface increases with company size. But also the probability for a malicious insider, probability for an accidental exposure, and the number of lost or stolen laptops, thumb drives, and backup drives, all increase with the number of employees.

We also find that the proportion of vendors that have outsourced cybersecurity varies by company size and this is important for the kind of due-diligence and remediation activities that we recommend.

We have therefore organized staffing level due-diligence by company size.

Due-Diligence

For due diligence described below, it is assumed that **cumulative-probability** has already been measured for your company and that management has set **cumulative-probability** goals. **Cumulative-probability** was measured by gathering headcounts and calculating probabilities for all of your current vendors that met the **PII-Threshold** (see below) and could expose your data[6].

Vendors with 1 to 650 Employees

For small vendors, outsourcing cybersecurity is common. When we gather headcount data on a vendor, we cannot determine if cybersecurity is outsourced, only that the company does not appear to have any internal certified cybersecurity employees. The following table is a breakdown of the percentage of companies by size range that would seem to have no internal cybersecurity[7].

Number Employees	With Internal Cybersecurity	With Audit & Compliance
1 to 50	1%	0%
50 to 200	22%	0% to 12%
200 to 650	50%	15% to 36%

Due-diligence activities for these small vendors amounts to determining **1)** if they have outsourced, **2)** whether this outsourced cybersecurity is ongoing, **3)** the qualifications of the people performing internal or outsourced cybersecurity and **4)** the number of hours per year of cybersecurity support the vendor is receiving.

[6] Contact VivoSecurity for a cumulative risk assessment.
[7] Source of data is VivoSecurity

Steps Activities

1 Determine that the vendor will have the potential to expose an amount of PII that is over some predetermined threshold (**PII-Threshold**). This threshold should be determined in consultation with management. An example threshold might be PII records for 500[8] people or more.

Consider if **exposure-reduction**[9] can be achieved at low-cost and weigh this cost against the cost of due-diligence which includes: **1)** the initial due-diligence, **2)** periodic reassessments, **3)** contract negotiations and enforcement, and **4)** ensuring that data is purged when the vendor contract is terminated.

2 If the number of PII records is over the **PII-Threshold** and exposure-reduction is not an initial option, submit the vendor name and URL to obtain an ***On-demand Report*** from VivoSecurity (see details above and example in the Appendix).

Evaluating Internal Security

3 If the ***On-demand Report*** report reveals any CISSP certified employees, consider that the vendor has strong, ongoing, cybersecurity[10] and a low probability for data breach. Proceed to evaluate Cumulative-Risk (step-6 below).

4 If the vendor appears to have no cybersecurity (zero employees with CISSP certification), contact the vendor and determine if they do have internal cybersecurity and what the qualifications are of the people supporting cybersecurity.

We recommend creating a list of criteria that the TPRM team deems acceptable (see examples in the Appendix). For example, a list of other acceptable certifications or years of experience in cybersecurity (we only use CISSP because it is most common – many other certifications are just as valuable or even better). We recommend assessing the person's qualifications through a short phone interview, asking predetermined questions.

If the vendor does have internal cybersecurity from a person with strong qualifications as determined by the TPRM team, consider that the vendor has strong, ongoing, cybersecurity and a low probability for data breach. Proceed to evaluate Cumulative-Risk (step-6 below).

Evaluating Outsourced Security

5 If the vendor has outsourced cybersecurity, then the TPRM team should determine how many hours per year of ongoing support is received, and the qualifications of the people performing the support. The TPRM team should determine in advance the number of hours they deem adequate as a function of company size. For example, the TPRM team might determine that 20 hours per month for a company with 100 employees is

[8] For many states, companies must report a data breach if more than 500 people are affected.
[9] ***Exposure reduction*** reduces the impact, if a data breach were to happen. Examples of exposure reduction might be anonymizing data, encrypting a database or reducing the amount of data that could be exposed.
[10] Some TPRM teams may prefer to verify the employees anyway and even interview the certified employees to confirm their qualifications and experience.

adequate. We provide an example table in the appendix that is based upon the average number of CISSP for companies in the size range of 2,000 employees.

If the people providing the support don't have a CISSP certification, then the TPRM team should use the same approach as in step 4 above to assess qualifications.

Evaluating Cumulative-Risk

6 Management should decide ahead of time, the cumulative-probability for data breach that is acceptable. These cumulative-probability goals should be decided by data breach size and documented. We describe this process in our previous white paper[11].

The effect of this potential vendor on maintaining these cumulative-probability goals should be evaluated using small data breach sizes, for example 1,000 and 10,000 people affected, and the ***On-demand Report*** will include new cumulative-probability forecasts which include this potential vendor.

A revised ***On-demand Report*** should be requested if there is new information from due-diligence or if there are remediation requirements. The revised ***On-demand Report*** will then reflect the revised effect on cumulative-probability (see column-6 in the table from the Vendor-S example below).

For example, if due-diligence reveals that the company does have on-going internal cybersecurity and the person has experience equivalent to a CISSP certification, then a revised ***On-demand Report*** should be requested showing one CISSP headcount.

If remediation requires changes to the cybersecurity headcount, the revised ***On-demand Report*** will also show the change in probability and cumulative-probability as a result of remediation, which can be used for KPIs as explained below.

If the cumulative-probability goals cannot be met, either:

- Some kind of **exposure-reduction**[12] should be required for this vendor, which reduces the amount of data that could be exposed to below the **PII-Threshold** in step-1,
- Another vendor should be dropped or **exposure-reduction** performed on another vendor[13],
- Management should be notified and sign-off on new cumulative-probability goals.

Remediation[14]: if the qualifications of internal or external cybersecurity support do not meet the TPRM team's documented standards, this should be addressed in the contract. The contract

[11] How to Improve Third-Party Risk Management using Statistical Models, D. Hann & T. Lee

[12] **Exposure reduction** reduces the impact, if a data breach were to happen. Examples of exposure reduction might be anonymizing data, encrypting a database or reducing the amount of data that could be exposed.

[13] Since cumulative-probability is from the number of vendors (sum of probabilities across vendors), addressing another vendor can achieve the same goal of reducing cumulative-probability.

[14] **Remediation** is the process of addressing problems that were discovered during due-diligence. Addressing problems will mitigate risk from a third-party data breach. These steps could be things that the vendor must do, such as increasing cybersecurity consulting hours or steps that your company must take such as anonymizing data shared with a vendor.

might require that the internal cybersecurity employee obtain a certification that the TPRM team determines is adequate, or that the hours of the cybersecurity consultant be increased, or that a different cybersecurity consultant be used that is more qualified.

The contract: we recommend that the contract requires maintaining a certain level of on-going internal cybersecurity support, or an equivalent level of ongoing external cybersecurity support. The contract should allow periodic post-contract due-diligence to verify that this same level of internal or external cybersecurity support is present. If external cybersecurity is used, the contract should allow you to directly contact the cybersecurity consultant and ask questions about the vendor's security. The contract should also anticipate that the number of employees might increase and that cybersecurity support should also increase. Written verification of data purge should be required upon contract termination.

TPRM Effectiveness (KPIs): calculate effectiveness as the percent change in cumulative-probability for small data breaches which results from remediation activities. The change in cumulative-probability can be obtained from the updated version of the ***On-demand Report*** from VivoSecurity that includes the changes to certification headcounts or consulting hours required in the contract (see column-7 in the table from the Vendor-S example below). The percent change to cumulative-probabilities should then be summed across all new vendors with executed contracts.

For example, in one quarter, if vendor-contracts were signed for two new vendors and due-diligence and remediation reduced probability by 20% for each vendor for a data breach affecting 1,000 people, then remediation efforts should be reported as reducing cumulative-probability by a total of 40% for a data breach affecting 1,000 people.

Example, Reducing a small vendor’s impact on cumulative-risk

Step-1, PII-Threshold met, Step-2 Report Requested.

A company that has already been assessed for cumulative-risk, is considering a new vendor, Vendor-S for the processing of data. The TPRM team reached out to the department that is sponsoring Vendor-S and discovered that the vendor would have access to PII data for 10-million people. The TPRM team also learned that exposure-reduction would be a costly process to implement. Management’s **PII-Threshold** is 500-people over 2-years, so the **TPRM cybersecurity expert** requested an ***On-demand Report*** from VivoSecurity. VivoSecurity required only the vendor’s name.

Step-3, No CISSP

The report showed that Vendor-S had about 150 employees, with no CISSP or CISA certified employees, so potentially no internal cybersecurity. This data was collected without the help or knowledge of Vendor-S.

The **TPRM cybersecurity expert** observed that the Vendor-S website showed they had Soc 2 type-1 and NIST CSF assessments, so it came as a surprise that they would have no internal cybersecurity. It is likely that Vendor-S had contracted out cybersecurity which is acceptable, since probability for data breach increases with company size and Vendor-S is small. Also only 20% of companies this size have internal cybersecurity.

Step-4, TPRM team due-diligence

The **TPRM cybersecurity expert** phoned Vendor-S and learned that Vendor-S had engaged a cybersecurity consultant for a limited time to obtain the Soc 2 type-1 and NIST CSF assessments. The assessments were reassuring but not sufficient considering the number of employees that Vendor-S has and the amount of PII data that could be exposed.

Step-5, Evaluating Outsourced Security

In a phone call with the consultant who was engaged to help Vendor-S obtain their assessments, the **TPRM cybersecurity expert** determined that the consultant was well qualified and had a CISSP certification, along with many other certifications. The NIST CSF and Soc 2 type-1 assessments for Vendor-S were also good evidence of the consultants abilities.

Item	Result
Exposure	10-Million people affected
Employees	150
Cybersecurity	Outsourced, limited engagement
Remediation	Ongoing 10-hours per week, CISSP-level cybersecurity consultant
Contract	● copy of signed contract with CISSP-contractor ● notification if contract changes ● right to contact CISSP-contractor.
KPI	32% & 16% reduction in cumulative-probability for 1K & 10K data breach

The **TPRM cybersecurity expert** required a minimum of 10-hours per week of on-going support from a consultant with a CISSP certification. The **TPRM cybersecurity expert** generated this requirement quickly and objectively, based upon a table created ahead of time, very similar to Table-1 in the Appendix.

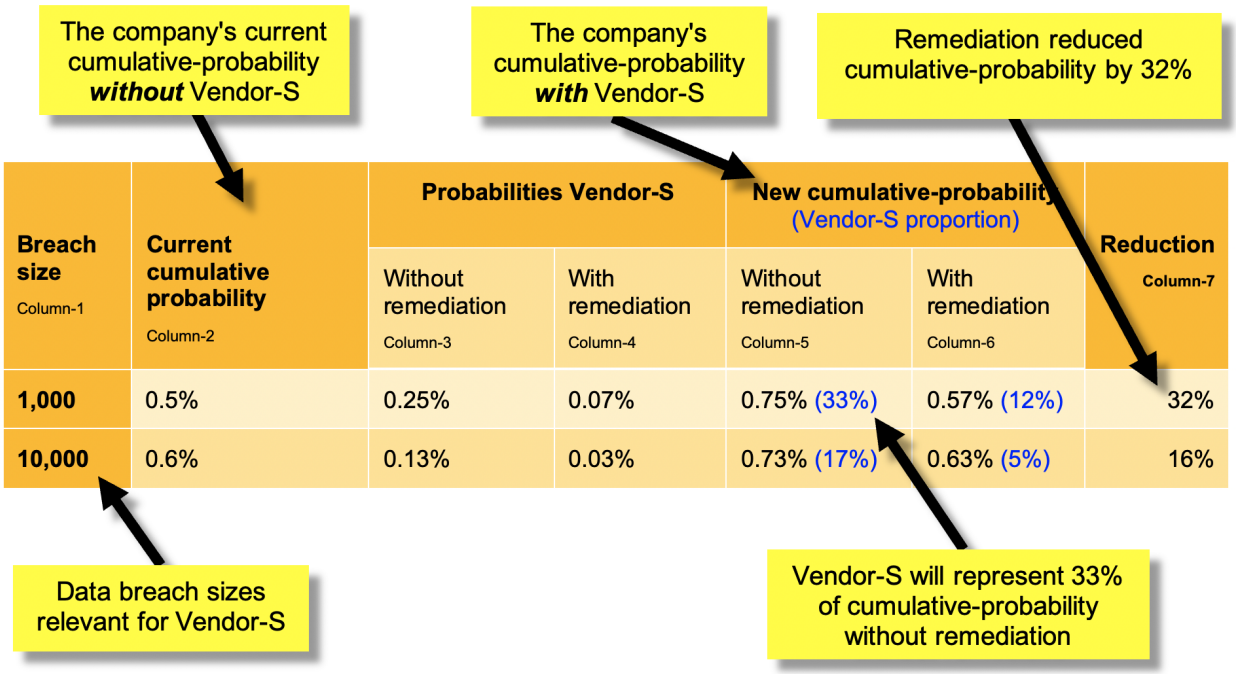
At this point, due-diligence was finished and remediation would be handled by the legal team through the vendor-contract. The due-diligence for Vendor-S was straightforward, objective, quick to complete and did not require a tedious review of controls. Remediation was reasonable from the perspective of Vendor-S, did not attempt to micromanage Vendor-S' cybersecurity, could be quantified, was science based and not a matter of opinion, and the **TPRM cybersecurity expert** was satisfied that current or future risks would be well managed by a qualified cybersecurity expert. Contract requirements were also straightforward and easy to understand, could be quickly fulfilled and the vendor was on-boarded with minimal delay.

Remediation: Continuous engagement of a cybersecurity consultant with a CISSP certification, minimum of 10-hours per week.

Contract: Required a copy of the signed contract with a cybersecurity-consultant which guaranteed 10-hours per week of the consultant's time. Vendor-S must provide notification if there is a change to the cybersecurity-consultant's contract. Vendor-S granted the right to contact the cybersecurity-consultant regarding hours and the state of cybersecurity for Vendor-S anytime over the period of the vendor-contract.

TPRM Effectiveness (KPIs): Generating the ***On-demand Report*** for Vendor-S was a two step process. In the second step, the TPRM team notified VivoSecurity that Vendor-S would have a quarter of a CISSP headcount going forward as part of remediation (10-hours per week is equivalent to a quarter of a CISSP headcount). The revised ***On-demand Report*** therefore included the table below, which shows: cumulative-probabilities for the company, before and after Vendor-S, with and without remediation. The table also presents the reduction in cumulative-probabilities that result from remediation. This reduction can be used as a more meaningful ***Key Performance Indicator*** (KPI) for the TPRM team.

Following is a description of the table and how it can be used to measure the value of remediation.



Breach size Column-1	**Current cumulative probability** Column-2	**Probabilities Vendor-S**		**New cumulative-probability** (Vendor-S proportion)		**Reduction** Column-7
		Without remediation Column-3	With remediation Column-4	Without remediation Column-5	With remediation Column-6	
1,000	0.5%	0.25%	0.07%	0.75% (33%)	0.57% (12%)	32%
10,000	0.6%	0.13%	0.03%	0.73% (17%)	0.63% (5%)	16%

Column-1 shows that Vendor-S is evaluated at two data breach sizes: 1,000 and 10,000 people affected. These sizes were chosen because they are larger than the number of employees for Vendor-S and more likely to be the vendor's customer's data. Smaller data breaches were not considered since the most likely small data breach for Vendor-S is simply an exposure of their internal HR records. The table does not include larger data breach sizes because cumulative-probability tends to be dominated by much larger companies and the percent reduction for Vendor-S would not be significant. This trend can already be seen in the table, since Vendor-S' proportion of cumulative-probability drops from 33% to 17% (column-5) as data breach size increases from 1-thousand to 10-thousand people affected.

Column-2 shows that the company's current cumulative-probability without Vendor-S is very good at 0.5% and 0.6% for 1000 and 10,000 people affected, respectively. This was calculated by simply summing the probabilities across vendors that could expose the companies PII data. VivoSecurity had this information from a previous assessment of all vendors that could expose an amount of PII data over the **PII-Threshold**.

Column-3 shows that the probability for Vendor-S, without any remediation, is 0.25% and 0.13%. At first this might seem very good, but these probabilities must be added to the companies current cumulative-probability in **column-2**. **Column-5** shows that this new cumulative-probability would be 0.75% and 0.73% – which is a substantial increase in cumulative-probability.

For remediation, the TPRM team recommended 10-hours per week of CISSP consulting time. This might seem like a lot, but it only represents a quarter of a cybersecurity employee and Vendor-S does have the potential to expose records for 10-Million people. **Column-4** shows the value of this quarter-headcount: the probability for Vendor-S becomes 0.07% and 0.03%. **Column-6** shows that when this new probability is added, cumulative-probability increases to a more acceptable 0.57% and 0.63%. **Column-7** shows that the TPRM team's efforts have therefore resulted in a 32% and 16% reduction in cumulative-probability over what it would have been without their efforts (32% = (0.75% - 0.57%) / 0.57%).

These percentages for Vendor-S can be summed across all vendors on-boarded within a quarter and reported as a more meaningful measure of the TPRM value per quarter.

Cumulative-Risk: The company chose aggressive cumulative-risk goals. Adding Vendor-S, with requested remediation, did not impact these goals.

Vendors with 650 to 5,000 Employees

For midsized companies, outsourcing cybersecurity is rare and a good reason to choose a different vendor or justify exposure-reduction.

The following table is a breakdown of the percentage of companies by size range that would seem to have no internal cybersecurity[15].

Number Employees	With Internal Cybersecurity	With Audit & Compliance
650 to 2,000	80%	60%
2,000 to 5,000	95%	70% to 80%

Companies in this size range are also more likely to have audit/compliance employees, and empirical modeling finds these employees to be just as important as cybersecurity employees at reducing portability for data breach. So an absence of audit/compliance employees is another reason to choose a different vendor or justify exposure-reduction.

Due-diligence activities for these medium sized companies amounts to **1)** determining if they have outsourced security, **2)** perform peer comparisons to evaluate security, and **3)** determine if cumulative-risk goals can be met.

Steps **Activities**

1 Determine that the vendor will have the potential to expose an amount of PII that is over some predetermined threshold (**PII-Threshold,** see above**)**.

[15] Source of data is VivoSecurity.

Consider if exposure-reduction can be achieved at low-cost and weigh this cost against the cost of due-diligence which includes: **1)** the initial due-diligence, **2)** periodic reassessments, **3)** contract negotiations and enforcement, and **4)** ensuring that data is purged when the vendor contract is terminated.

2 If the number of PII records is over the **PII-Threshold** and exposure-reduction is not an initial option, submit the vendor name and URL to obtain an ***On-demand Report*** (see details above and example in the Appendix) from VivoSecurity.

Evaluating Security

3 If the vendor has no CISSP, contact the vendor and determine if they do have internal cybersecurity and what the qualifications are of the people supporting cybersecurity.

We recommend creating a list of criteria that the TPRM team deems acceptable. For example, a list of other acceptable certifications or years of experience in cybersecurity (we only use CISSP because it is most common. Many other certifications are just as valuable or even better). We recommend assessing the person's qualifications through a short phone interview with predetermined questions.

If the vendor has outsourced cybersecurity, or has a cybersecurity team with insufficient experience or training, consider that the vendor presents too much risk. Consider that exposure-reduction is the only option unless the vendor is willing to internalize cybersecurity with a sufficient number of cybersecurity and audit/compliance employees.

4 If the vendor has an internal cybersecurity team, perform peer comparisons to evaluate the vendor's security. When comparing with peers, consider data breach sizes larger than the number of employees for the vendor. For example, if the vendor has 1,000 employees, use a data breach size of 10,000 people affected to compare the company with peers.

If the vendor has a weak cybersecurity compared with peers as judged by probability for PII data breach and will not consider increasing cybersecurity audit/compliance headcount, the vendor presents too much risk. Consider that exposure-reduction is the only option.

Evaluating Culture

5 Empirical regression modeling finds that audit/compliance certified employees are just as effective at reducing probability for data breach as cybersecurity employees. This makes sense, since many data breaches are caused by employees not following policies and procedures, or by a lack of policies and procedures. We interpret the presence of audit/compliance certified employees as a measure of management's desire to have and follow good policies and procedures.

Most companies with 2,000 employees or more have certified audit/compliance specialists. If the vendor has no certified audit/compliance specialists, consider that the vendor presents too much risk. Consider that exposure reduction is the only option unless the vendor is willing to address its weak audit/compliance posture by increasing

the number of trained and experienced people at a level deemed acceptable by the TPRM team.

Evaluating Cumulative-Risk

6 Management should decide the cumulative-probability of data breach that is acceptable. These cumulative-probability goals should be decided by data breach size and documented. We describe this process in our previous white paper[16]. Meeting these cumulative-probability goals will be an important consideration for companies in this size range.

The effect of this potential vendor on maintaining these cumulative-probability goals should be evaluated using data breach sizes larger than the number of employees for the vendor. For example, 10K, 100K and 1M people affected should be considered for a vendor with 2,000 employees. The ***On-demand Report*** will include the new cumulative-probability forecasts which include this potential vendor (see column-5 in the table for Vendor-M example below).

A revised ***On-demand Report*** should be requested if there is new information from due-diligence found in step 3 and 5 above, or if there will be headcount changes agreed upon in the contract that are a result of remediation. The revised ***On-demand Report*** will then reflect the revised effect on cumulative-probability if there are corrections to the existing headcounts (see column-5 in the table for Vendor-M example below) and if there changes due to remediation (see column-6 in the table for Vendor-M example below).

For example, if due-diligence reveals that the company does have on-going internal cybersecurity and the person has experience equivalent to a CISSP certification, then a revised ***On-demand Report*** should be requested with one CISSP headcount.

If the cumulative-probability goals cannot be met, either:

- Some kind of exposure-reduction should be required for this vendor, which reduces the amount of data that could be exposed to below the **PII-Threshold** in step-1,
- Another vendor should be dropped or exposure-reduction[17] performed on another vendor,
- Management should be notified and sign off on new cumulative-probability goals.

Remediation: if cybersecurity is found to be outsourced then require that cybersecurity be internalized with a sufficient number of certified cybersecurity, audit/compliance employees. For companies that will not internalize cybersecurity or will not increase headcounts to a level deemed satisfactory by the TPRM team, consider exposure-reduction, avoidance, or dropping another vendor or exposure-reduction for another vendor. Remember that third party data breach risk is a cumulative-risk so reducing the risk from another vendor is a legitimate way to meet cumulative-risk goals.

[16] How to Improve Third-Party Risk Management using Statistical Models, D. Hann & T. Lee

[17] **Exposure reduction** reduces the impact, if a data breach were to happen. Examples of exposure reduction might be anonymizing data, encrypting a database or reducing the amount of data that could be exposed.

For companies with 2,000 or more employees that do not have an audit/compliance specialist, require obtaining such a specialist, either by hiring a new employee or by incentivising an existing employee to get certified.

The contract: If an increase in cybersecurity, audit/compliance headcounts is agreed upon, then the vendor should commit to maintain these higher levels, as well as maintaining higher ratios, even as the vendor grows. No specific contract requirements will be needed for future due-diligence since headcounts can be verified without the vendor's assistance.

TPRM Effectiveness (KPIs): calculate effectiveness as the percent change in cumulative-probability for small data breaches which results from remediation activities. The change in cumulative-probability can be obtained from the up-dated version of the ***On-demand Report*** from VivoSecurity that includes the changes to certification headcounts or consulting hours required in the contract (see column-7 in the table for Vendor-M example below). The percent change to cumulative-probabilities should then be summed across all new vendors with executed contracts.

Example, Addressing a midsized vendor's culture weakness

Step-1, PII-Threshold met, Step-2 Report Requested.

A company that has already been assessed for cumulative risk, is considering a new vendor, Vendor-M to host a SaaS application. The TPRM team reached out to the department that is sponsoring Vendor-S and discovered that the vendor would have access to PII data for 10-million people. The TPRM team also learned that exposure-reduction would be a costly process to implement. Management's **PII-Threshold** is 500 records over 2-years, so the **TPRM cybersecurity expert** requested an ***On-demand Report*** from VivoSecurity. VivoSecurity required only the vendor's name.

Step-3, Internal Cybersecurity

Data for Vendor-M was collected without the help or knowledge of Vendor-M and the report showed that Vendor-M had about 1,500-employees, with 1-CISSP and 0-CISA certified employees. Vendor-M website shows they have Soc 2 type-2 and they also have a NIST CSF assessment and an ISO 27001/2.

Step-4, Peer Comparisons

The bubble chart below, which was included in the ***On-demand Report,*** shows the frequency of data breach among companies of similar size, including Vendor-M. Increased fraction of experienced and certified-trained cybersecurity employees is indicated by increased circle sizes. Decreased fraction of experienced and certified-trained audit/compliance employees is indicated by darker circle colors. Probability for data breach affecting 10-thousand people is indicated on the Y-axis, with low probability at the top of the axis, high probability at the bottom of the axis. It should be noted that if probability is once in one-thousand, it should be understood to mean that a data breach would occur every year among 1000 similar companies, or once in ten-years among 100 similar companies,

The graph shows Vendor-M to be among the highest risk companies, with a 1%[18] annual probability for a data breach affecting 10,000 people.

Step-5, Evaluating Culture

Many companies that are smaller have a larger cybersecurity team and most companies the size of Vendor-M have at least one CISA certified employee.

Considering that Vendor-M had no CISA certified employees, **the TPRM team will require a CISA certified employee**. Remember, CISA certified employees are just as effective at reducing probability for PII data breaches as CISSP certified employees.

It may seem hard to convince a vendor to obtain a CISA certified employee, but when confronted with a peer comparison that shows they have one of the weakest cybersecurity headcounts, when you explain that they will represent 33% of your cumulative-probability for a data breach affecting 10K people because of their weak security (see table below), and knowing other customers may be similarly worried, Vendor-M may budget for a CISA – just to support sales.

Item	Result
Exposure	10-Million people affected
Employees	1,500
Cybersecurity	1-CISSP, 0-CISA
Remediation	Acquire 1-CISA
Contract	● Acquire 1-CISA within 6-months ● Maintain 1-CISA & 1-CISSP during contract period & notification if change ● Notify within 30-days if major non-compliance incident.
KPI	27% reduction in cumulative-probability for 10K data breach

But the TPRM team is not requiring that Vendor-M hire a new employee, they could just as well incentivize an existing employee to obtain their CISA certification, which is a much easier certification to obtain than the very technical CISSP. Likely an existing employee will jump at the opportunity, and likely Vendor-M may even have training budgets to support the certification.

Some TPRM teams might be inclined to also specify requirements around reporting structure. For example, require that the CISA report to someone in the C-suit, but not report to the CIO, or CISO – two groups that are important to audit. Since vendors might resent micromanaging their org-chart, the same goal might be accomplished by requiring reporting of major compliance

[18] 1% annual probability is the same as once in 100-years, on average.

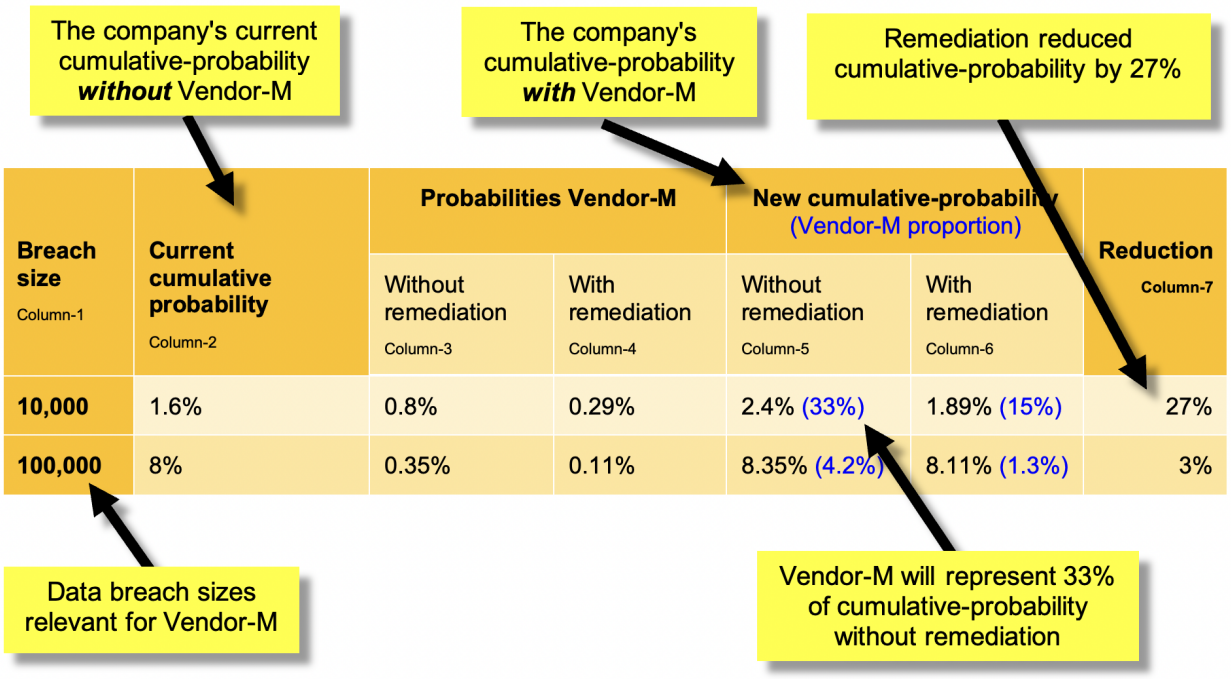
incidents. Contract negotiations should then cover what constitutes a reportable compliance incident.

Remediation: Hire one CISA certified employee, or have an existing employee obtain a CISA certification.

Contract: Require a CISA certified employee within the next 6-months. Maintain at least one CISSP certified employee and one CISA certified employee, during the period of the contract. Vendor-M must provide notification if there is a change to the employment status of the CISSP or CISA certified employees. Vendor-M must provide notification of any major non-compliance incidents within 30 days. Verification of data purge is required upon contract termination.

TPRM Effectiveness (KPIs): Generating ***On-demand Report*** for Vendor-M was a two step process. In the second step, the TPRM team notified VivoSecurity that the contract would require one CISA certified employee. The updated ***On-demand Report*** therefore included the table below, which shows the value of remediation for Vendor-M and can be used as a more meaningful ***Key Performance Indicator*** (KPI) for the TPRM team.

Following is a description of the table and how it can be used to measure the value of remediation.



Breach size Column-1	Current cumulative probability Column-2	Probabilities Vendor-M		New cumulative-probability (Vendor-M proportion)		Reduction Column-7
		Without remediation Column-3	With remediation Column-4	Without remediation Column-5	With remediation Column-6	
10,000	1.6%	0.8%	0.29%	2.4% (33%)	1.89% (15%)	27%
100,000	8%	0.35%	0.11%	8.35% (4.2%)	8.11% (1.3%)	3%

Column-1 shows that Vendor-M was evaluated at two data breach sizes: 10,000 and 100,000 people affected. These sizes were chosen because they are larger than the number of employees for Vendor-M and more likely to be the vendor's customer's data. Smaller data breaches were not considered since the most likely small data breach for Vendor-M is simply an exposure of their internal HR records. The table does not include larger data breach sizes because cumulative-probability tends to be dominated by much larger companies and the

percent contribution for Vendor-M would not be significant. Indeed, the report shows that Vendor-M would represent a minor portion of cumulative-probability at 100,000 people affected.

Column-2 shows that the company's current cumulative-probability without Vendor-M is 1.6% and 8% for 10,000 and 100,000 people affected, respectively[19]. This was calculated by simply summing the probabilities across vendors that could expose the companies PII data. VivoSecurity had this information from a previous assessment of all vendors that could expose an amount of PII data over the **PII-Threshold**.

Column-3 shows that the probability for Vendor-M, without any remediation, is 0.8% and 0.35%. At first this might seem very good, but these probabilities must be added to the companies current cumulative-probability in **column-2**. **Column-5** shows that this new cumulative-probability would be 2.4% and 8.35% – which is a substantial increase in cumulative-probability for a data breach affecting 10,000 people. In fact, Vendor-M by itself, would represent 33% of the cumulative-probability (33% = 0.8%/2.4%) for this data breach size.

After due-diligence, the TPRM team recommended one CISA certified employee. **Column-4** shows the value of the employee: the probability for Vendor-M becomes 0.29% and 0.11%. **Column-6** shows that when this new probability is added, cumulative-probability increases to a more acceptable 1.89% and 8.11%. **Column-7** shows that the TPRM team's efforts have therefore resulted in a 27% and 3% reduction in cumulative-probability over what it would have been without their efforts (27% = (2.4% - 1.89%) / 1.89%).

These percentages for Vendor-M can be summed across all vendors on-boarded within a period of time and reported as a more meaningful measure of the TPRM value per quarter

Cumulative-Risk: The company chose industry median cumulative-risk goals. Even with Vendor-M obtaining an additional CISA certified employee, Vendor-M will cause the company to fail to meet their goals. Cumulative-risk goals were decided by a committee as described in our earlier white paper. In many companies and in this company, this committee meets every week to consider all third party risks, from all vendors that are being considered or revisited as part of on-going due-diligence. The ***TPRM team manager*** obtained approval to on-board Vendor-M, and temporarily exceed cumulative-risk goals, but with a commitment to reduce cumulative-risk goals through exposure-reduction with another vendor. The CFO is part of the committee and approved a small budget to implement the exposure-reduction.

Vendors with more than 5,000 Employees

For companies over 5-thousand employees, 100% have internal cybersecurity teams and most have audit/compliance teams[20].

Number Employees	With Internal Cybersecurity	With Audit & Compliance
5,000 +	100%	92% to 99%

For these large companies, due-diligence will be focused on peer comparisons and meeting cumulative-risk goals.

[19] The reason cumulative-probability is so high at 100,000 people affected is because there are more vendors, mostly large vendors, with higher probabilities that contribute at that data breach size.
[20] Source of data is VivoSecurity.

Steps **Activities**

1 Determine that the vendor will have the potential to expose an amount of PII that is over some predetermined threshold (**PII-Threshold**). This threshold should be determined in consultation with management. An example threshold might be PII records for 500 people or more.

Consider if exposure-reduction can be achieved at low-cost and weigh this cost against the cost of due-diligence which includes: **1)** the initial due-diligence, **2)** periodic reassessments, **3)** contract negotiations and enforcement, and **4)** ensuring that data is purged when the vendor contract is terminated.

2 If the number of PII records is over the PII-Threshold and exposure-reduction is not an initial option, submit the vendor name and URL to obtain an ***On-demand Report*** (see details above and example in the Appendix) from VivoSecurity.

Evaluating Security

3 If the vendor has no CISSP, consider that the vendor presents too much risk. Consider that exposure reduction is the only option unless the vendor is willing to address its cybersecurity with increasing the number of trained and experienced people at a level deemed acceptable by the TPRM team.

4 If the vendor has an internal cybersecurity team, perform peer comparisons to evaluate the vendor's security. When comparing with peers, consider data breach sizes larger than the vendor. If the vendor has a weak cybersecurity compared with peers as judged by probability for PII data breach and will not consider increasing cybersecurity audit/compliance headcount, the vendor presents too much risk. Consider that exposure-reduction is the only option.

Evaluating Culture

5 Empirical regression modeling finds that audit/compliance certified employees are just as effective at reducing probability for data breach as cybersecurity employees. This makes sense, since many data breaches are caused by employees not following policies and procedures, or by a lack of policies and procedures. We interpret the presence of audit/compliance certified employees as a measure of management's desire to have and follow good policies and procedures.

If the vendor has no certified audit/compliance specialists, consider that the vendor presents too much risk. Consider that exposure reduction is the only option unless the vendor is willing to address its weak audit/compliance posture by increasing the number of trained and experienced people at a level deemed acceptable by the TPRM team.

Evaluating Cumulative-Risk

6 Management should decide the cumulative-probability of data breach that is acceptable. These cumulative-probability goals should be decided by data breach size and

documented. We describe this process in our previous white paper[21]. Meeting these cumulative-probability goals will be an important consideration for companies in this size range.

The effect of this potential vendor on maintaining these cumulative-probability goals should be evaluated using data breach sizes larger than the number of employees for the vendor. For example, 100K, 1M and 10M people affected should be considered for a vendor with 20,000 employees. The ***On-demand Report*** will include the new cumulative-probability forecasts which include this potential vendor.

A revised ***On-demand Report*** should be requested if there is new information from due-diligence found in step 3 and 5 above, or if there will be headcount changes agreed upon in the contract.

The revised ***On-demand Report*** will then reflect the revised effect on cumulative-probability. For example, if due-diligence reveals that the company does have on-going internal cybersecurity and the person has experience equivalent to a CISSP certification, then a revised ***On-demand Report*** should be requested with one CISSP headcount.

If the changes are from remediation, or exposure reduction, the revised ***On-demand Report*** will also show the change in probability and cumulative-probability as a result, which can be used for KPIs as explained below (see column-6 in the table for Vendor-L example below).

If the cumulative-probability goals cannot be met, either:

- Some kind of exposure-reduction should be required for this vendor, which reduces the amount of data that could be exposed to below the **PII-Threshold** in step-1,
- Another vendor should be dropped or exposure-reduction[22] performed on another vendor,
- Management should be notified and sign off on new cumulative-probability goals.

Remediation: An increase in cybersecurity, audit/compliance headcounts, dropping another vendor, or exposure-reduction such as anonymizing data, or encryption, or reducing the amount of data exposed.

The contract: If an increase in cybersecurity, audit/compliance headcounts is agreed upon, then the vendor should commit itself to maintain these higher levels, as well as maintaining higher ratios, as the vendor grows. No specific contract requirements will be needed for future due-diligence since headcounts can be verified with a new ***On-demand Report***. Verification of data purge is required upon contract termination.

TPRM Effectiveness (KPIs): calculate effectiveness as the percent change in cumulative-probability for small data breaches which results from remediation activities. The

[21] How to Improve Third-Party Risk Management using Statistical Models, D. Hann & T. Lee

[22] **Exposure reduction** reduces the impact, if a data breach were to happen. Examples of exposure reduction might be anonymizing data, encrypting a database or reducing the amount of data that could be exposed.

change in cumulative-probability can be obtained from the up-dated version of the ***On-demand Report*** from VivoSecurity that includes the changes to certification headcounts or consulting hours required in the contract (see column-7 in the table for Vendor-L example below). The percent change to cumulative-probabilities should then be summed across all new vendors with executed contracts.

Example, Assessing & addressing the risk from a very large vendor

Step-1, PII-Threshold met, Step-2 Report Requested.

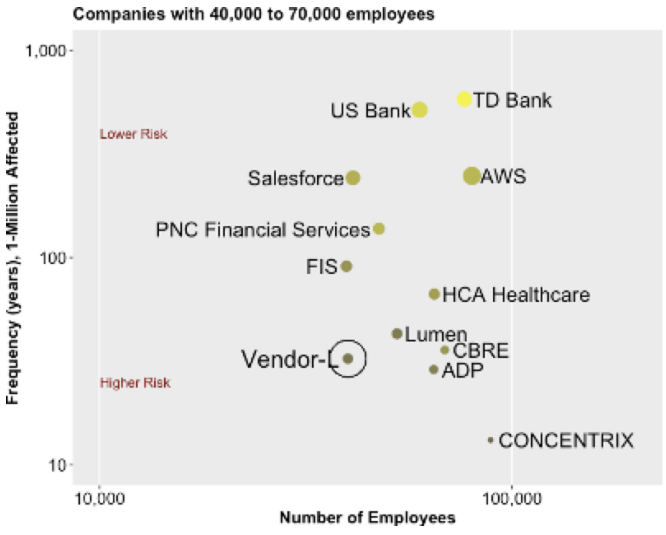
Vendor-L is being considered for IaaS, to host a database. The database would hold data on 10-million people. Management's **PII-Threshold** is 500 records over 2-years, so VivoSecurity prepared an ***On-demand Report*** requiring only the vendor's name.

Step-3, Internal Cybersecurity

The ***On-demand Report*** shows that Vendor-L has about 40,000 employees, with 75-CISSP, 15-CISA certified employees. Vendor-L's website shows a strong SOC 2 assessment, ISO 27001/2 and apparently mature cybersecurity. But a peer comparison finds that Vendor-L is below average for the probability for PII data breach among companies of similar size.

Item	Result
Exposure	10-Million people affected
Employees	40,000
Cybersecurity	75-CISSP, 15-CISA, among highest probability within peer group.
Remediation	Exposure-reduction
Contract	No cybersecurity related requirements
KPI	109%, 150%, 133% & 200% cumulative-probability reduction for 100K, 1M, 10M & 100M affected data breach size, respectfully.

The bubble chart, which was included in the ***On-demand Report,*** shows the frequency of data breach among companies of similar size, including Vendor-L. Increased fraction of experienced and certified-trained cybersecurity employees is indicated by increased circle sizes. Decreased fraction of experienced and certified-trained audit/compliance employees is indicated by darker circle colors. Probability for data breach affecting 1-Million people is indicated on the Y-axis, with low probability at the top of the axis, high probability at the bottom of the axis. It should be noted that if probability is once in one-thousand, it should be understood to mean that a data breach would occur every year among 1000 similar companies, or once in ten-years among 100 similar companies,



Step-4, Peer Comparisons, Step-5 Evaluating Culture

The bubble chart shows that Vendor-L to be among the highest risk companies, with a 3%[23] annual probability for a data breach affecting 1-Million people. The graph shows that many companies that have a lower probability have larger audit/compliance headcounts.

Step-6, Evaluating Cumulative-Risk

A vendor that would appear to have a mature cybersecurity would cause cumulative-risk goals not to be met. If Vendor-L was onboarded with no remediation, it would cause cumulative-risk to nearly double for larger data breach sizes (see column-5 in the table below) – and the vendor is too large to expect any changes to its cybersecurity.

Vendor-L demonstrates that if your company wants to reduce third-party data breach, it is important to measure the cumulative-risk even for large vendors with mature cybersecurity.

The TPRM team recommends either:

- Revising cumulative-risk goals
- Considering a different vendor
- Exposure-reduction by encrypting the database that will be hosted with Vendor-L

Management chose exposure-reduction. Costs associated with running an encrypted database will be borne by the department that owns the application that will use the database.

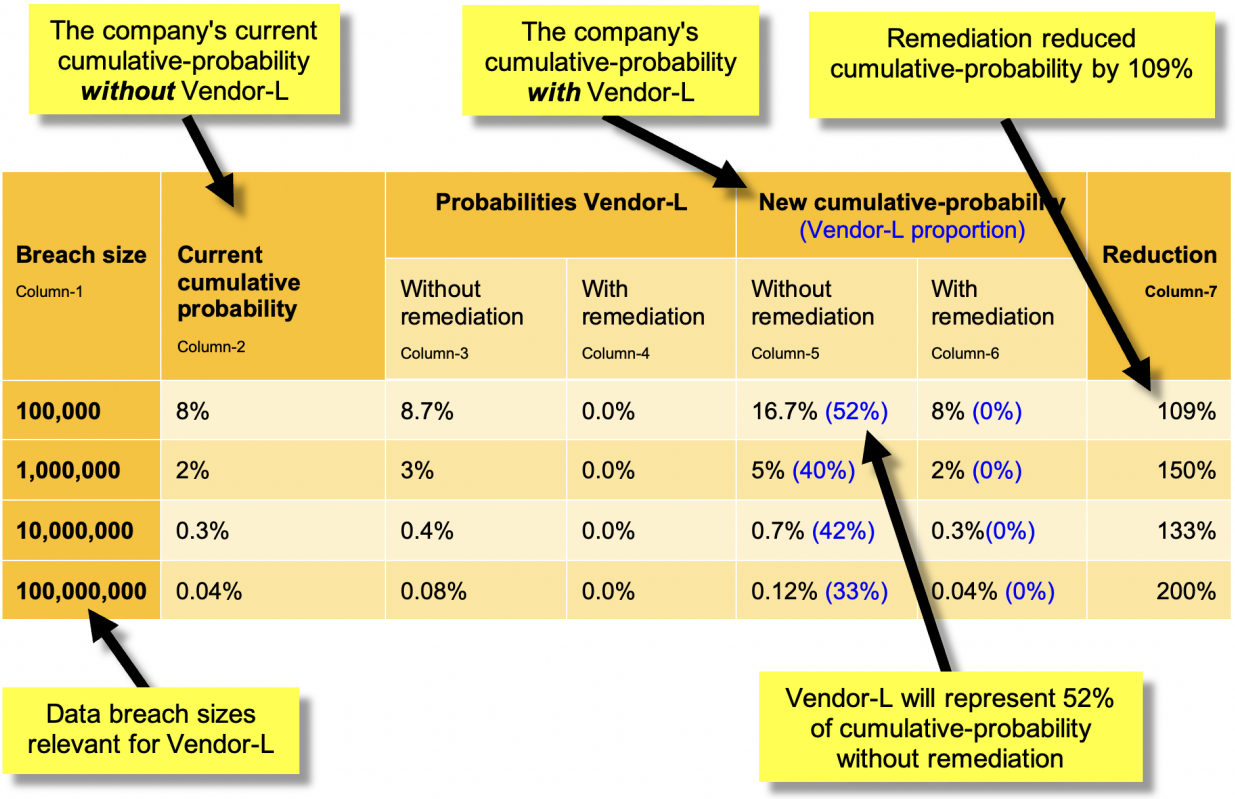
Remediation: Work with the database owner to budget for and implement encryption.

Contract: No requirements related to cybersecurity.

TPRM Effectiveness (KPIs): In this example, the ***On-demand Report*** for Vendor-L was just a one step process. The initial ***On-demand Report*** included the table below, which shows the value of remediation if the risk from Vendor-L was completely eliminated through exposure-reduction, and can be used as a more meaningful *Key Performance Indicator* (KPI) for the TPRM team.

Following is a description of the table and how it can be used to measure the value of remediation.

[23] 3% annual probability is the same as once in 33-years, on average.



Breach size Column-1	**Current cumulative probability** Column-2	**Probabilities Vendor-L**		**New cumulative-probability** (Vendor-L proportion)		**Reduction** Column-7
		Without remediation Column-3	With remediation Column-4	Without remediation Column-5	With remediation Column-6	
100,000	8%	8.7%	0.0%	16.7% (52%)	8% (0%)	109%
1,000,000	2%	3%	0.0%	5% (40%)	2% (0%)	150%
10,000,000	0.3%	0.4%	0.0%	0.7% (42%)	0.3%(0%)	133%
100,000,000	0.04%	0.08%	0.0%	0.12% (33%)	0.04% (0%)	200%

Column-1 shows that Vendor-L was evaluated at four data breach sizes: 100K, 1M, 10M and 100M people affected. These sizes were chosen because they are larger than the number of employees for Vendor-L and more likely to be the vendor's customer's data. Smaller data breaches were not considered since the most likely smaller data breach for Vendor-L is simply an exposure of their internal HR records.

Column-2 shows that the company's current cumulative-probability without Vendor-L is 8%, 2% 0.3% and 0.04% for 100K, 1M, 10M and 100M people affected, respectively. This was calculated by simply summing the probabilities across vendors that could expose the companies PII data. VivoSecurity had this information from a previous assessment of all vendors that could expose an amount of PII data over the **PII-Threshold**.

Column-3 shows that the probability for Vendor-L, without any remediation, is 8.7%, 3% 0.4% and 0.08%. Without any remediation, these probabilities should be added to the current cumulative-probabilities if Vendor-L is onboarded. **Column-5** shows that this new cumulative-probability would be 16.7%, 5%, 0.7% and 0.12% – which is a substantial increase in cumulative-probability. In fact, Vendor-L by itself, would represent more than 52% of the cumulative-probability for a data breach affecting 100K people (see percentages in blue).

The ***On-demand Report*** is often a two step process, but in the first step the table above is generated assuming due-diligence will result in complete exposure-reduction and **column-4** shows probabilities of zero assuming complete exposure-reduction. **Column-6** shows these zero probabilities added to the current cumulative-probabilities (column-2) and of course Vendor-L will represent 0% of the cumulative-probabilities with complete exposure-reduction (see percentages in blue).

Column-7 shows that the TPRM team's efforts have therefore resulted in a 109%, 150%, 133% and 200% improvement in cumulative-risk over what it would have been without their due-diligence and remediation (109%=(16.7%-8%)/8%). In this example, remediation was directed internally, requiring encryption of the database that will be hosted with Vendor-L

These percentages for Vendor-L can be summed across all vendors on-boarded within a period of time and reported as a more meaningful measure of the TPRM value.

Cumulative-Risk: Vendor-L would have doubled cumulative-risk without exposure-reduction, causing cumulative-risk goals not to be met. With exposure-reduction cumulative-risk was unchanged and cumulative-risk goals were met.

Acknowledgements

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

Axel Troike

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.

Aaron Arutunian

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.

Shawn Wilde

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.

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.

Get a PDF version of this white paper

Appendix

Glossary

Exposure-reduction	Activities to reduce the impact if a data breach were to occur. Examples include reducing the amount of data that the vendor has access to, anonymizing data, encrypting a database that resides on the vendor's servers
Avoidance	Reduce cumulative-probability by not using a vendor.
Cumulative-Probability	Probability for a PII data breach across all vendors that could expose PII data. Usually calculated by data breach size since probability is a strong function of data breach size.
Cumulative-Risk	Cumulative-probability across all data breach sizes.
Cumulative-Frequency	The inverse of cumulative-probability.
Empirical regression model	A statistical model where input factors (explanatory variables) were discovered and not based upon theory or assumptions.
PII	Any kind of non-public ***Personal Identifiable Information*** that would trigger various state and federal reporting requirements. Non-public PII includes CHD (card holder data), PHI (protected health information) and PFI (personal financial data).
PII-Threshold	A maximum amount of PII, below which the vendor will not be included in cumulative-risk calculations. This maximum threshold should be set by management.
Remediation	The process of addressing issues found during vendor due-diligence.

Example, On-Demand Single Vendor Report

On Demand Report on Discover Financial Services

Data Breach Forecast

Peer Comparison

and effect on

Cumulative-Probability

for

Anonymous

an assessment based upon Certification level

An in-depth review by VivoSecurity for
Third Party Risk Management Teams

February, 2022

VIVO
VivoSecurity

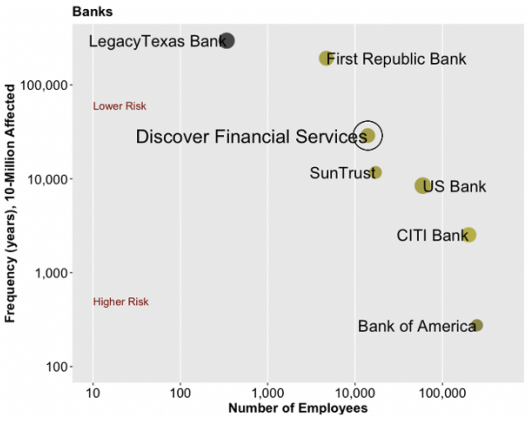
We have assessed the probabilities for PII data breach for ***Discover Financial Services*** and the effect of these probabilities on the cumulative-probabilities for ***Anonymous***. Empirical regression modeling has found that the number of employees overall and the number of employees with certain certifications is very predictive for PII data breach. Data breaches forecast by our model are all reportable PII data breaches such as 1) those caused by a **Malicious Outsider**, which can include network intrusion and infiltration of an email account; 2) by a **Malicious Insider**, which can include contractors, past employees and current employees; 3) by **Accidents** which can include emailing sensitive data to the wrong client or potential data exposure due to misconfiguration of an application or server; and 4) by **Lost or Stolen** electronic devices including laptops, thumb drives and tape drives, misplaced, stolen or lost in transit.

Model inputs are the total number of employees and the normalized headcounts (count of the number of employees divided by the number of IT employees) of certain certifications found to be predictive. These certification headcounts have the additional value of providing insights into the vendor's cybersecurity spending and management culture. These certifications (see Appendix for more detail) are 1) the **CISSP** cybersecurity certification, which can be interpreted as a measure of cybersecurity-spend, training and experience; 2) the **CISA** audit certification, which can be interpreted as a measure of management's commitment to enforcing good policies and procedures and 3) the **MCSA** certification, which is the most common Microsoft certification and which can be interpreted as a measure of management's commitment to hiring certified and trained employees in general.

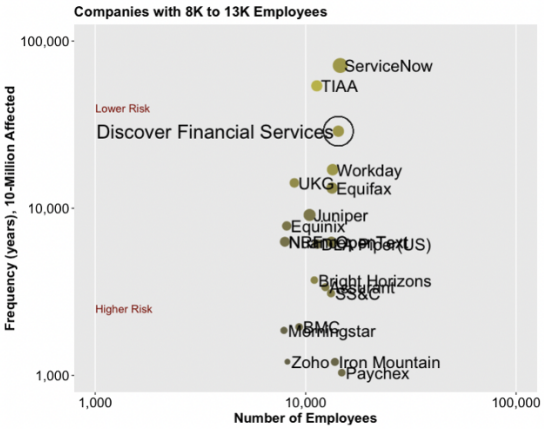
We find that data breach risk significantly increases with the total number of employees and statistically is mitigated by the number of certified cybersecurity, compliance, audit and IT professionals as a proportion of IT size. The fraction of certified professions must increase faster than the total number of employees in order to maintain the same level of risk. In other words, to have the same probabilities for data breach, a company with 10-thousand employees must have a higher percentage of CISSP, CISA and MCSA, than a company with 1-thousand employees.

We have performed two peer comparisons: industry peers and a cross-industry size peers. The peer comparisons were performed at a data breach affecting 10-million people since it is very hard for larger companies to prevent smaller data breaches and the effect of a robust cybersecurity posture is best seen at larger data breach sizes.

We find that Discover Financial Services is about typical for probability of a data breach affecting 10-million people, both among industry peers and among size peers, due to a typical number of CISSP and CISA headcount for their company size (see table 1).



Graph 1, Frequency of data breach among peer group, based upon company size and the number of cybersecurity and compliance employees. Increased fraction of experienced and certified-trained cybersecurity employees is indicated by increased circle sizes. Decreased fraction of experienced and certified-trained compliance employees is indicated by darker circle colors.



Graph 2, Cross Industry Comparison for Frequency of data breach, based upon company size and the number of cybersecurity and compliance employees.

Number Employees	CISSP	CISA	MCSA	Date	1K	10K	100K	1M	10M	100M
13,986	76	59	13	11/11/2020	2.3%	0.75%	0.23%	0.052%	0.0035%	0.00042%
14,300	68	49	12	2/11/2022	2.9%	1.02%	0.34%	0.083%	0.0061%	0.00080%
	NA	NA	NA	Corrections	NA	NA	NA	NA	NA	NA
	NA	NA	NA	Remediations	NA	NA	NA	NA	NA	NA

Table 1, Total number of non-contract employees and employees with three predictive certifications for Discover Financial Services, for two points in time. Corrections are any corrections to headcounts found during due-diligence by Anonymous, and Remediations are any changes to headcount due to remediation activities by Anonymous.

We have collected data on Discover Financial Services two times over the past year and we find that during this time the company has grown in the number of employees even as the number of cybersecurity (CISSP) and Audit/compliance (CISA) employees has been reduced. Empirical regression modeling finds that these employees are especially important at preventing large data beach and we find that the probability for large data breach (10M and 100M affected) has nearly doubled as a result of the headcount changes.

Table 2 shows the effect of Discover Financial Systems on cumulative-probabilities for Anonymous. We find that the vendor will have a small effect on cumulative-probabilities over the range of data breach sizes that we think are appropriate (100K to 100M people affected). We also find little value in exposer-reduction for this vendor.

Breach size Column-1	Current cumulative Probability Column-2	Probabilities for Discover Financial Systems		New cumulative-probability (Discover Financial Systems proportion)		Reduction Column-7
		Without remediation Column-3	With remediation Column-4	Without remediation Column-5	With remediation Column-6	
1,000	3.5%	2.9%	0.0%	6.40% (45%)	3.5% (0%)	83%
10,000	1.6%	1.0%	0.0%	2.62% (39%)	1.6% (0%)	64%
100,000	8%	0.34%	0.0%	8% (4%)	8% (0%)	4%
1,000,000	2%	0.083%	0.0%	2% (4%)	2% (0%)	4%
10,000,000	0.3%	0.0061%	0.0%	0.31% (2%)	0.3% (0%)	2%
100,000,000	0.04%	0.00080%	0.0%	0.04% (2%)	0.04% (0%)	2%

Table 2, The effect of **Discover Financial Systems** on cumulative-probabilities. **Column-1** shows that the new vendor was evaluated at six data breach sizes, but we recommend considering sizes 100K, 1M, 10M and 100M people affected since these sizes are larger than the number of employees and more likely to be the vendor's customer's data since the most likely small data breach is simply an exposure of their internal HR records. **Column-2** shows the company's current cumulative-probability without the new vendor. This was calculated by simply summing the probabilities across vendors that could expose the companies PII data. VivoSecurity has this information from a previous assessment of all vendors that could expose an amount of PII data over the **PII-Threshold**. **Column-3** shows that the probability for the new vendor, without any remediation. If there is no remediation, these probabilities should be added to the current cumulative-probabilities if the new vendor is onboarded. **Column-5** shows that this new cumulative, which is a small increase in cumulative-probability for larger data breach sizes. In fact, the new vendor by itself, would represent 4% or less of the cumulative-probability for a data breaches affecting 100K people and more (see percentages in parentheses). The ***On-demand Report*** is often a two step process, but in the first step the table above is generated assuming due-diligence will result in complete exposure-reduction and **column-4** shows probabilities of zero assuming complete exposure-reduction. **Column-6** shows these zero probabilities added to the current cumulative-probabilities (column-2) and of course the new vendor will represent 0% of the cumulative-probabilities with complete exposure-reduction. If exposure-reduction is perused, **Column-7** shows the value of the TPRM team's efforts, which is the reduction cumulative-risk over what it would have been without their due-diligence and remediation. The value is small for data breaches affecting 100,000 and more people.

Model Accuracy

Accuracy of the model itself can be established by extending the analysis to all of your vendors, including ones that cannot expose your data. With a large pool of vendors, the history of data breaches often matches the future forecast, and this can give you a notion of accuracy. Also, across a large pool of vendors, the future frequency of data breach is often high, for example 5 data breaches per year, allowing a shorter period of time to further test the accuracy of the model.

Model accuracy can also be established at the time of model development. One way to judge model accuracy is the proportion of all companies that account for 50% of data breaches. An inaccurate model (the null model) would predict that 50% of data breaches would occur among 50% of all companies. A perfect model that could identify the very companies that will experience a data breach next year would identify 0.04% of companies that will account for 50% of data breaches. Our empirical regression model which is based upon headcounts, can identify 0.4% of companies that will account for 50% of data breaches.

Example Qualifications and Consulting Hours

Other certifications or experience considered equivalent or better than CISSP

- Five or more years of experience working as a cybersecurity professional
- Certified Information Security Manager (CISM)

Table-1, Example minimum CISSP consulting time for companies that have outsourced cybersecurity. Hours are based upon the average CISSP headcount for companies with 2000 employees. The source of data is VivoSecurity.

Number of Employees	Hours per week
50	6
100	12
150	18
200	24
250	30
300	36
350	42
400	48