



Leveraging Breach Statistics to Re-Focus Third Party Monitoring

September 2026



Our Approach

ONE

Calculating the Likelihood of a Breach

TWO

Third Party Population Management

THREE

Modern Risk Management

FOUR

Q&A

Presenter



BOB MOONEY

Manager, Crowe
Cyber / TPRM



Calculating the Cost of a Breach

The Study

*Crowe professionals were lucky enough to attend a local ISACA LA chapter event with a discussion and analysis of a publicly available whitepaper by Timothy Smith, CPA, CPA/CITP, CISA and Thomas Lee, PhD. titled: **Third-Party Data Breach- What are the odds?***

- The whitepaper leverages data from breach events related to **reportable PII**
- The whitepaper also provides us with instructions and considerations for running the study on **our own organizations**. *This comes down to two data points:*
 - # of third parties in our inventory
 - Likelihood of a breach for **every third party in our inventory(!!!)**
- ***But where do we start?*** There is no one-size-fits-all approach to determining the likelihood that a breach will occur at a single third party, much less every third party we have
- Luckily, the whitepaper gives us a place to start

Find the whitepaper referenced in today's presentation [here.](#)

The Study

Critical Equations – Two Ways to Get There. We could sum the probabilities of each individual third party in our inventory experiencing a breach. That sounds hard.

$$E = \sum_{n=1}^N P_n$$

Expected Value
(Breaches per year)

Alternatively, what if we knew the ***average probability*** a third party would experience a breach?

$$E = N \times P_{ave}$$

Expected Value
(Breaches per year)

Find the whitepaper referenced in today's presentation [here](#).

The Magic Number

Luckily, they did the work – analyzing publicly reported breach data to find the **average probability a third party will experience a breach.**

$$P_{\text{ave}} = 0.066\%$$

Find the whitepaper referenced in today's presentation [here.](#)

A quick poll...

1. Do you have a single, inventoried your third party population? How many?
2. Do you classify third parties by tier?



Find the whitepaper referenced in today's presentation [here.](#)

Then What?

Let's see how **our probability** of experiencing a third party breach changes based on **our third party population**.

# of Third Parties (N)	P _{ave}	Likelihood (E) = N x P _{ave}	What we can expect
50	0.066%	3.3%	1 breach every 30 years
500	0.066%	33%	1 breach every 3 years
1,000	0.066%	66%	1 breach every 1.5 years
5,000	0.066%	330%	~3 breaches per year

For organizations with large third party footprints, this expected breach frequency is an unacceptable risk.

Find the whitepaper referenced in today's presentation [here](#).

Limitations

Let's take a step back. While the study serves as a great place to start, we must remember that we all work for unique organizations with our own complex third party footprints.

- Some third parties handle more than just PII
 - Non-regulated data being exposed, altered (integrity), or unavailable may also result in downstream impact
 - This could mean lost competitive advantage, or productivity lost to re-work
- Other cyber risks such as direct connections (e.g. VPN) are not considered
- Other third parties may not handle much sensitive data, but a lack of availability would be a huge issue
- The study acknowledges certain limitations in sample data used to determine P_{ave} , such as:
 - <500 records – below breach reporting threshold
 - Data handled by third party is obfuscated or encrypted
 - Inactive third parties where data *should be* purged

Before we start discussing ways to *reduce* our likelihood of significant exposure in the event that we experience a third party breach...

Find the whitepaper referenced in today's presentation [here](#).



Population Management

Population Management – Who is *in* ‘N’?

Let's refine our third party classifications so we can focus our time and effort on our largest points of exposure. For which third party types is an outage, loss of integrity, or breach unacceptable?

Start with a **complete and accurate** inventory (or as close as we can get):

- How many third parties handle regulated data (our ‘N’ value)?
- Do we know how many records they handle?
- Of all the data points we can capture, what **traits / characteristics** does our TPRM function need to focus on?

Inherent risk questionnaires are a **critical tool** for validating the third party relationship information (including data types & volume shared). IRQs:

- Capture key risk factors
- Enhance stakeholder accountability
- Support the consistent risk-rating of third parties
- Enable organizations to focus on the third parties most likely to experience a breach

Population Management – Who is *in* ‘N’?

Continuing from the prior slide...

Class	% Makeup (of third party population)	Traits
Critical	5%	• Access to customer or regulated data (PII, PHI, etc.) • Access to highly-confidential internal data • Strict uptime / availability requirements • Data integrity has significant downstream impact
High	15%	
Moderate	40%	• Access to non-reportable quantities of regulated data • Access to proprietary or confidential internal data
Low	40%	• Access to somewhat-sensitive internal data • Support non-critical internal operations
Exempt & Out-of-Scope	N/A	• Gov. Entities • Mandated by Customer • Contractor leveraging a virtual desktop • Managed by Contract

Note: ‘% Makeup (of third party population)’ reflects a typical third party breakdown that Crowe typically observes across client third party populations.

Population Management – Preparing for the Worst

Once our class definitions are appropriately applied across our population, we can appropriately prepare for the potential downstream impact of a breach.

Class	% Makeup (of third party population)	Breach Impact
Critical	5%	- Significant downstream operational, financial, compliance, and/or reputational impact - Unable to resume or maintain operations - Loss or exposure is material
High	15%	- Elevated downstream operational, financial, compliance, and/or reputational impact - Difficult to resume or maintain operations - Loss or exposure may be material
Moderate	40%	- Some non-cyber downstream impact - Cumbersome or lengthy recovery - Lost productivity
Low	40%	- Short-term recovery - Potentially some lost productivity
Exempt & Out-of-Scope	Variable	Should always be negligible , or risk/responsibility avoided

Population Management – Our New ‘N’

Let's look back at the likelihood of experiencing a breach, focusing on **who** matters

Class	% Makeup (of third party population)	# of Third Parties (N)	P _{ave}	Likelihood (E) = N x P _{ave}	What we can expect
Critical	5%	50	0.066%	3.3%	1 breach every 30 years
High	15%	150	0.066%	9.9%	1 breach every 10 years

We're left with a realistic estimate of our likelihood of experiencing a third party breach, which we can prepare for.



Modern Risk Management

Modern Risk Management

We now understand our third party inventory, but how do we appropriately manage it? Who should we focus on to make sure we use our limited time and resources managing risk.

Class	% Makeup (of third party population)	Treatment
Critical	5%	- Continuous cyber monitoring, TPRM prioritizing alerts - At least annual due diligence and/or validation of key trust documentation. - Increased scrutiny of contractual terms related to data & system security - Formalized & enforced data destruction, return, expiration requirements - Non-cyber monitoring (financial health, reputational, or compliance issues)
High	15%	
Moderate	40%	- Continuous cyber monitoring - Periodic due diligence, potentially reduced scope/depth - Non-cyber monitoring (financial health, reputational, or compliance issues)
Low	40%	- Continuous cyber monitoring - Ad-hoc or alert-based due diligence - Non-cyber monitoring (financial health, reputational, or compliance issues) as deemed necessary
Exempt & Out-of-Scope	Variable	May consider non-cyber monitoring (financial health, reputational, or compliance issues)

Modern Risk Management

TPRM isn't always in the business of telling relationship owners how to work with a third party, but we can provide suggestions and warnings.

- Self-Regulating our Exposure
 - Do they need this data?
 - Can we limit the fields shared?
 - Who has the (encryption) keys?
 - Can it be accessed in an alternative way? *Virtual machines, (your) company-issued laptops*
 - Do multiple third parties provide a similar service and/or handle the overlapping sets of data?
- Consideration as a Target
 - Does anyone care? *Would a breach result in a minor annoyance, or would we lose \$ and customers?*
 - Is the third party under social scrutiny?
 - Is the third party widely known?



Q&A



Thank you



Bob Mooney

Bob.Mooney@Crowe.com

"Crowe" is the brand name under which the member firms of Crowe Global operate and provide professional services, and those firms together form the Crowe Global network of independent audit, tax, and consulting firms. "Crowe" may be used to refer to individual firms, to several such firms, or to all firms within the Crowe Global network. Crowe Cayman Ltd., C3 India Delivery Centre LLP (formerly known as Crowe Horwath IT Services LLP), and ITR Economics LLC are subsidiaries of Crowe LLP. Crowe LLP is an Indiana limited liability partnership and the U.S. member firm of Crowe Global. Services to clients are provided by the individual member firms of Crowe Global, but Crowe Global itself is a Swiss entity that does not provide services to clients. Each member firm is a separate legal entity responsible only for its own acts and omissions and not those of any other Crowe Global network firm or other party. Visit www.crowe.com/disclosure for more information about Crowe LLP, its subsidiaries, and Crowe Global.

The information in this document is not – and is not intended to be – audit, tax, accounting, advisory, risk, performance, consulting, business, financial, investment, legal, or other professional advice, and should not be relied upon as such. Some firm services may not be available to attest clients. The information is general in nature, based on existing authorities, and is subject to change. The information is not a substitute for professional advice or services, and you should consult a qualified professional adviser before taking any action based on the information. Crowe is not responsible for any loss incurred by any person who relies on the information discussed in this document. © 2026 Crowe LLP.