Aggregated Vendor Risk—the Cyber Security Blind Spot

A Vendor Assessment Paradigm Change is Urgently Needed

Feb, 2020

Angelina Yang, David Zelinger and Thomas Lee Ph.D.

Companies across industries and company sizes are relying on 3rd parties for evermore business critical functions, yet the process of evaluating, quantifying and managing 3rd and 4th party risk continues to rely on maturity and compliance based scoring methodologies. These methodologies fail to capture the true risk to the enterprise—the risk from the sheer number of vendors. This *aggregated* risk is significant, accounting for approximately 50% of a company's large data breach risk. We argue for evaluating vendor risk in the same way financial portfolio risk is managed, from the standpoint of *probability*, a method which better captures the large, several orders of magnitude differences between vendors and allows quantifying and managing aggregated vendor risk.

Companies in all industries are relying on hundreds, sometimes thousands, of vendors to manage the complexity of today's business landscape. This web of vendors can include suppliers, contractors, SaaS, PaaS and IaaS.

This increasing access and movement of sensitive data across internal and external systems creates a significant and growing cyber security risk with about about 50% of large PII[1] data breaches caused by third parties[2]. An analysis of data breach costs finds that these third party breaches are just as impactful[3], causing significant business, reputational and operational impact. Third party risk is not limited to data breach. For the financial industry, 75% of Foreign Corrupt Practices Act (FCPA) cases resulted from third party partners[4].

Third party risk is therefore a significant portion of the enterprise risk. Cyber security teams apparently recognize this since a recent survey based study of the financial services industry[4] found that 75% of respondents reported that third party data breaches had or could potentially have critical business impact. Business also seem to understands the magnitude of the risk with over 90% of respondents answering that *Third Party Risk Management* (TPRM) programs report to the Boards of Directors at least once a year, and management level staff viewed cyber security, reputational and operational risk as the top three concerns when it came to third parties[4].

For companies that don't understand the importance of third party risk—beware, regulators are paying close attention to how firms are protecting client data. In 2019 alone, firms were fined millions of dollars for failing to properly monitor this risk[4] and there are ongoing changes in the regulatory landscape like the new European Banking Authority (EBA) Guidelines on Outsourcing Arrangements, the California Consumer Privacy Act (CCPA), General Data Protection Regulation (GDPR) and others are likely to result in increasing fines in 2020 and beyond unless there is significant improvement in TPRM programs.

But the current approach for measuring third party risk is inadequate, leaving a significant blind spot in managing overall cyber security risk. The process for measuring third party risk has been from the perspective of the cyber security practitioner. It consists largely of

---

[1] Personal Identifiable Information (PII), includes Protected Health Information (PHI), Card Holder Data (CHD) and Personal Financial Information (PFI).

[2] 40% of CHD, 67% of PHI data breaches affecting more than 100K people, data from VivoSecurity, 2018 and 2019

[3] See *Regression Model for the Impact of a Data Breach for a Financial Institution* Thomas Lee, Jason Hegland, Spencer Graves, Richmond fed research conference, 2018

[4] CeFPro 2019, *Third Party Risk: Chasing Maturity in a Dynamic Landscape*

maturity or compliance based scoring[5] methodologies[6], often manually assessed, most often based upon proprietary or opinion based weighting of security controls and configurations[7].

The problem with maturity or compliance scores is that your organization's risk is not from any single vendor, but the aggregated risk across all of vendors. A typical company has hundreds if not thousands of vendors and this aggregated risk can only be assessed with probabilities—not scores.

Applying basic statistical techniques to a theoretical *typical* large institution is illustrative of the problem's potential magnitude. If a third party has a probability for data breach of 1.6% (once in 62 years, on average), this may at first seem acceptable. But in an environment where there are potentially thousands of vendors engaged in the data supply chain, if only 50 have a 1.6% annual likelihood of a data breach, your chance of having a data breach among those 50 vendors is a concerning, once every 5 months, on average.

So, aggregate third party risk is a significant concern, and it cannot be assessed with scoring methodologies. The financial industry has the skill to understand this problem—they commonly apply principles of aggregated risk in assessing financial portfolios. Yet, the financial industry uses subjective scoring methodologies to assess third parties, just like all other industries. The question is why?

We propose, the reason is because third party assessments are driven by the cyber security practitioner. The cyber security practitioner views the problem from the very detailed and technical perspective of controls and compliance. In fact, compliance with security standards is the foundation of the cyber security practice. But accurate probability models cannot be easily developed when this kind of information cannot be collected across all companies that **have** and **have not** experienced data breach. Expert opinion for how these controls reduce probability is not a good substitute for sound model development practices; the scientific literature is robust on the inaccuracy of expert judgment when it comes to predicting rare events[8], and large data breaches are rare events for any particular company.

But there are factors that can be measured for all companies, which strongly and independently correlate with data breaches, and which allow generating accurate probability models that can be used to asses and manage aggregate risk. These models are sufficiently accurate to find orders of magnitude differences between third parties[9] and can even determine probability as a function of data breach size.

Importantly, these models can be developed from non-technical measures that bring interpretability to non-technical senior management and the board of directors. And, because models are based upon non-technical inputs and independent of security controls, these models will remain accurate even as technology and criminal methodologies change.

Third party assessments efforts are generally under resourced. A recent survey of cyber security practitioners[7] found that nearly 60% of survey respondents rated their TPRM program as immature and only 35% felt they were adequately resourced to measure or manage this risk. This is understandable considering that current methods are not able to address the actual risk from third parties: the aggregated risk.

---

[5] These are subjective scores based upon opinion of the value of certain standard controls and different from the probability derived scores used in the financial industry.

[6] These methodologies often assume there is a set security controls e.g. NIST or PCI, that should be implemented. Full compliance is often too burdensome, so companies are scored by the degree of compliance via questionnaires. Other methods assume measuring external configurations such as web and email servers capture the level of maturity.

[7] 78% of companies use internally scoring methodologies according to CeFPro 2019 *Third-party cyber risk forfinancial services: blind spots, emerging issues & best practices*

[8] See *Thinking, Fast and Slow* by Nobel Laurette Daniel Kahneman.

[9] These models can identify 0.4% of companies that will account for 50% of PII data breaches, compared with a perfect model that would identify 0.04% of companies.

But we have argued that as much as 50% of the enterprise risk is due to third parties. We propose that companies stop using maturity or compliance based scoring methodologies and instead use probability models based upon other predictive factors that can be measured for all companies, and that TPRM programs be resourced at a level consistent with the magnitude of the risk. We argue that models should be interpretable by managers and the board of directors and follow sound model development practices recommended by the Federal Reserve and Office of the Comptroller of the Currency (OCC)'s Supervisory Guidance on Model Risk Management – Bulletin SR11-7[10].

A paradigm change is needed as companies become ever more dependent on third party services.

Authors

Angelina Yang is currently VP of Quantitative Analytics and AI Development at Wells Fargo, and senior advisor to VivoSecurity. Angelina is FRM certified, has extensive experience in fraud, data breach and financial crime modeling, and is a pioneer in novel data sources and modeling techniques. She was an ACAMS panelist in 2019, 2020. The views of the author do not reflect the views of Wells Fargo.

David Zelinger is currently advising early stage FinTech firms on go-to-market strategy and product messaging. Previously he has served at the management level across a range of financial services market participants, including Deutsche Bank, IHSMarkit, Duco Technology and others, with a specialization in delivering solutions to complex operational and regulatory risk problems.

Thomas Lee is the CEO of 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.

For inquiries, contact: Hayden McKaskle
Hayden@ChannelMarketPartners.com

(615) 739-8151

[10] https://www.federalreserve.gov/supervisionreg/srletters/sr1107.pdf