Third-party security in the year 2030

March 2024

Introduction

The demands on third-party risk management programs are exponentially increasing, highlighting the need to broaden coverage while simultaneously deepening insight. Recent technological innovation has created new possibilities, but because these advancements have been directed towards automating traditional, survey-based processes, it has been challenging to realize the necessary transformation. Given the large-scale, innovation-led disruption to standard business processes that are foreseeable in the next five years, proactive thought and action is required even more.

To address this accelerating need for change will take a combination of technology and first principles thinking, returning to the fundamental objectives of third-party security: identification of risk in the third-party population; assessing risk so it can be prioritized; and taking the appropriate action to mitigate risk. By rethinking how to most effectively utilize available third-party data and having a clear understanding of the objectives, it becomes possible to achieve unprecedented outcomes with much greater efficiency.

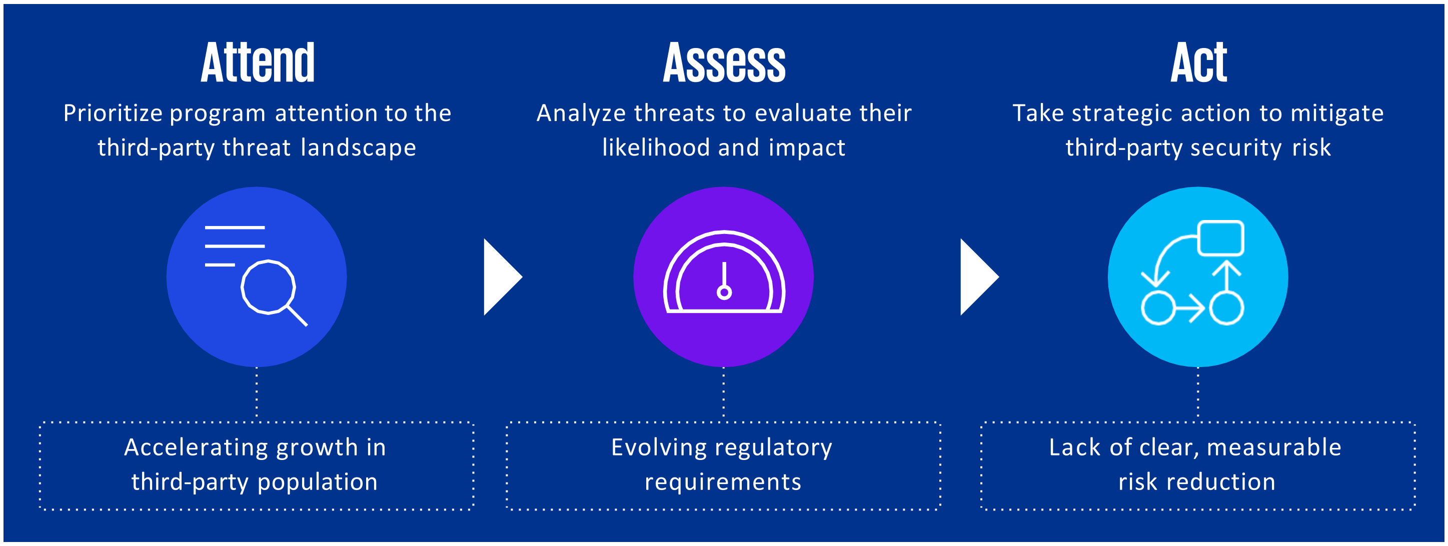
Uncover the transformational value of automation

To determine new directions forward, it is important to understand how existing processes came to be. Given the tools available and regulatory and compliance requirements to identify, assess, and manage risk, the approach commonly indicated was survey based. As the closest proxy for third-party risk assessment, questionnaires became the standard tool to assess third parties for security control implementation.

While the traditional approach has established strong awareness of the importance of third-party security and created a baseline framework for assessing risk, it has also led to a labyrinth of intricate processes, which are often siloed within organizations. Furthermore, risk management activity results often do not provide more granularity than whether a third-party has “passed” or “failed” assessment criteria. Without context as to the nature of the third-party relationship within an organization’s unique financial and risk environment, it is difficult to connect assessment outputs with bottom-line outcomes and drive tangible business decisions. Accordingly, the process can seem more like a box-checking exercise than true risk management for the stakeholders most involved.

It is understandable why the automation of these workflows is highly sought after and was the initial direction in applying technological innovation to this area. However, with the continually evolving and expanding third-party threat landscape, it is now widely understood that a shift towards continual, real-time monitoring is needed, which legacy processes cannot support, even with optimal workflow automation. Based on changing regulatory requirements already anticipating this shift, programs must begin to take action today.

Core processes must be reconsidered from first principles to unleash technological innovation to manage accelerating third-party risk, expanding coverage while deepening insight.



Attend

Prioritize program attention to the third-party threat landscape

Accelerating growth in third-party population

Assess

Analyze threats to evaluate their likelihood and impact

Evolving regulatory requirements

Act

Take strategic action to mitigate third-party security risk

Lack of clear, measurable risk reduction

Locating the right data for a data-driven approach

To understand what this change can look like and the transformational results that are possible, it is illustrative to look to how this has been manifested in other completely unrelated areas. Across industries, clear examples can be found of how new processes born out of today’s innovative technologies have delivered previously unthinkable value, with much more efficiency. In each case, the key characteristic of success has been the shift away from traditional “direct-data” methods where only one-to-one indicators of goals are considered, usually arrived at via surveys or top-down metrics created based on intuitive expectations. A metadata approach has been embraced in its place, where all accessible data is analyzed without preconceptions, to determine their correlations with clearly defined objectives.

The revolution in advertising and marketing strategy in recent years is a clear example of the results that can be realized from application of the metadata approach concept. While the traditional, focus-group method for developing and planning ad campaigns is still used, its previously central role has been supplanted. Customer insights were traditionally arrived at via a “direct-data” process that represented a very large investment, was limited to the topic set considered in the focus group, and was also difficult to generalize to the broader customer population. Today, marketers can rely on a potential customer’s metadata (age, location, search history, etc.) to predict interest and determine the optimal strategy. The transformational effectiveness of this approach is best demonstrated anecdotally: today, advertisements are so personal, specific, and timely, it often feels like cellphones must be continually monitoring private conversations. However, from the third-party risk management perspective, the reality—the power of machine-learning enabled statistical analysis of metadata—is crucial to understand.

Taking a similar example from a very different industry, traditionally professional sports decision-making was driven by “direct-data” indicators, characterized by a mixture of high-level summary statistics and coach intuition. It wasn’t until a first principles mindset was taken that embrace of a metadata-based approach began to be viewed as being fundamental to winning. Analysts asked the question, “Given the resources we have, how can we use them most effectively to produce wins?”

After looking at data with no presumptions other than clear focus on the objective, it turned out that the metrics and indicators predictive of success are very different from what conventional wisdom would suggest. Analysts were surprised to discover that expert intuition was frequently completely backward; the metrics identified as most correlated with the objective were completely undervalued, if tracked at all. There was initially significant pushback from industry leaders as to the value or justification of the new approach. However, given consistent, unprecedented results, best exemplified by the Chicago Cubs breaking their 100-year-old curse (winning the World Series in 2016), it has become the standard across sports[1].

Across industries, clear examples can be found of how new processes born out of today’s innovative technologies have delivered previously unthinkable value, with much more efficiency by shifting to a metadata approach.

Direct data approach

- Top down, intuition-based metrics
- Considers one-to-one indicators of goals
- Static, point-in-time insights
- Limited generality

Metadata approach

- Analysis without preconceptions
- Considers all indicators for contextual predictive value
- Dynamic, continual insights
- Broad applicability

[1] Source: Forbes, Jersey City, Abhas Ricky (Jan 31, 2019)

The broadened risk management horizon

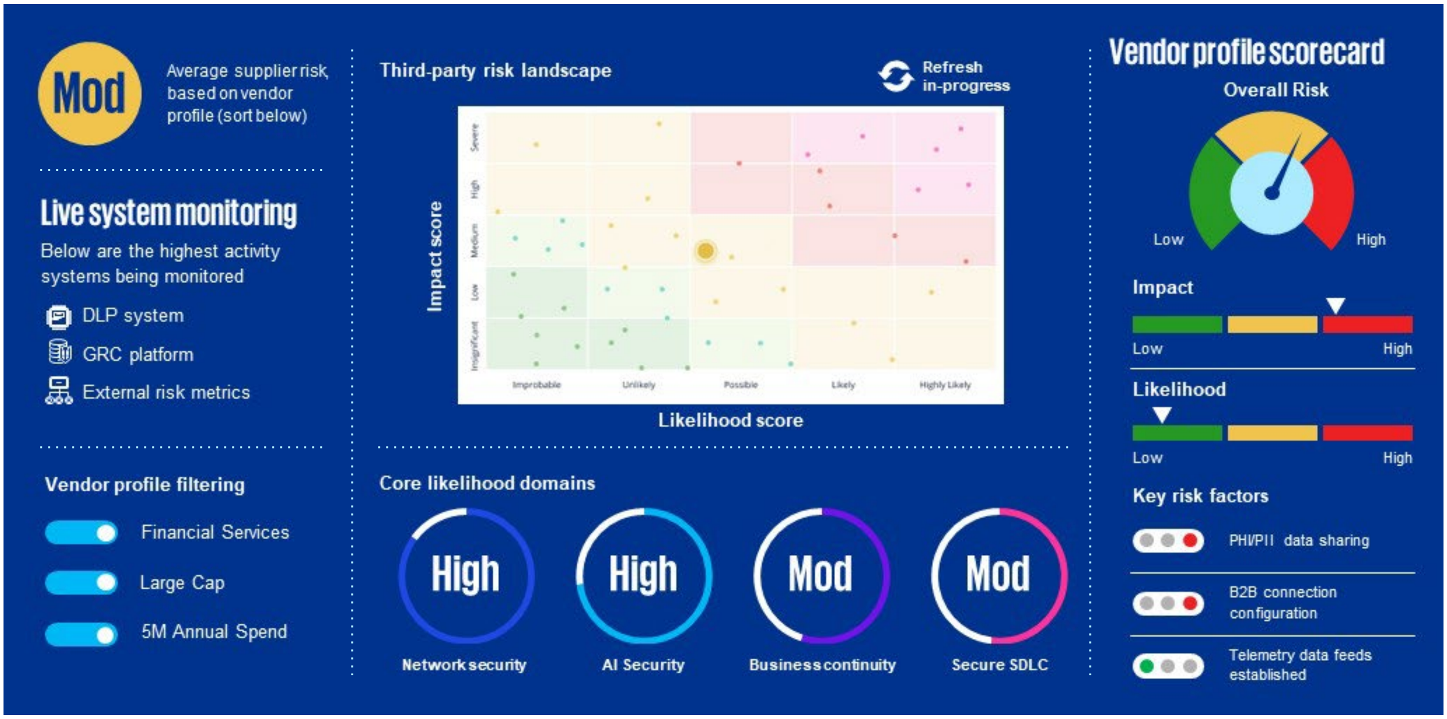
This shift from a “direct data” (survey-based) method to a “metadata” driven approach will also generate transformative results when applied to third-party risk management. Fundamentally, there are two dimensions to the overall risk a supplier poses: How much can a third-party hurt my organization with a breach? And how likely is a breach to occur? Aligned on these first principles and the core objectives of third-party risk management, the ways in which metadata can be utilized over traditional methods to determine the overall risk of a supplier can be identified.

The growth in useful data about third parties across internal and external data sources is constantly accelerating. However, as this abundance of data is continually being added on to a staggered pool of disconnected data sets, the value of this information is being lost. With a comprehensive strategy to consolidate data across sources so it can be analyzed for its explanatory and predictive power in the broadest possible context, previously unutilized data points can be used to provide meaningful risk metrics that inform strategic business decisions.

The concept of a risk-based, data-driven approach that is driven by machine learning begins to form that utilizes both internal and external data sources that are accessible for all vendors: for instance, sourcing and contracting information, external threat data, financial health information, business context metadata, among many more key data points. In this approach, with inputs for impact and likelihood stemming from metadata, any change to metrics results in real-time risk adjustment and analysis capability. This allows organizations to better understand the risk impact and likelihood across their entire vendor population for full-scale coverage.

An approach like this will tackle scalability and provide a more objective method to move beyond assessing risk in the vendor population to understanding the implications and necessary actions. It encourages less guessing and more accurate measuring, while facilitating real-time traffic monitoring across the network. Possibly most significantly, by linking them with metadata, continuous third-party risk metrics are never separated from the business environment that both informs them and that they in turn must inform. This targeted and evolving contextualized risk perspective allows monitoring activity to cascade down to specific business decisions, with measurable justification.

By leveraging machine learning to extract risk insight from consolidated internal and external live vendor data feeds, continuous, deep, and targeted coverage can be attained, as illustrated by the 2030 Vendor Dashboard.



Conclusion

A data-driven, intelligent automation enabled approach is already necessary to meet the present challenge third-party risk management programs are facing. However, as a result of the rate of technological change, it is possible to foresee that while it may seem to be very innovative and industry-leading today, it will become the standard within the next fiveyears.

As the technology in business environments continues to improve and expand, threat vectors will as well. The use of artificial intelligence/machine learning provides many paths forward for business improvement, but also opens a door to bad actors to find new routes of attack. The possibility of a technological ecosystem of zero-days every day comes to light in considering a world where malicious models are taught to look for weaknesses in infrastructure and constantly search for an entryway. With continual attempted attacks at a scale this large, a reactive, survey-based approach will not allow accurate prediction of the risk a third-party poses in a timely enough manner to allow for meaningful risk awareness and mitigating action. The capabilities for both real-time monitoring as well as predictive modeling will both be fundamental to third-party security in this environment, enabling the ability to proactively shift program resources to where they are most needed, based on real-time monitoring results.

Already, prevailing intuitions around the value of different aspects of the traditional process have been undermined by adjustments made during the COVID-19 pandemic. As organizations shifted away from performance of on-location, third-party risk assessments, opting for virtual substitutes, the value of face-to-face assessment has been called into question. Long after business has returned to normal, many large organizations have opted not to move back to on-location assessments. Similarly, with the increasing integration of augmented reality technology into the way business is conducted and life in general is lived, the entire survey-based approach will become less and less viable. As the understood value of in-person assessment was diminished during COVID-19, so will the trustworthiness of traditional approaches as a result of large-scale adoption of virtual and augmented reality. Increasingly, it will be clear that to attain reliable assurance of a third-party's security posture, objective data points must form the core of the assessment process.

Faced with these near-term developments, while a new approach to third-party risk management has been considered necessary for some time, adoption of it will soon expand beyond first-movers. As an intelligent automation enabled predictive modeling approach rooted in objective third-party data becomes increasingly seen as tangibly possible and able to deliver the needed scalability and insight, today's "cutting edge" may become tomorrow's baseline requirement faster than is realized. Based on a clear understanding of the fundamentals of third-party risk management and guided by the way similar strategic use of technology and data has delivered across industries, organizations must take informed steps now to ensure they are prepared.

8.9%

Very few World Economic Forum respondents surveyed indicate belief that generative AI will advantage cyber security defenders

Source: World Economic Forum, Cologny, Gretchen Bueermann et al., Jan 11, 2024

92 million

By 2030, the number of global digital jobs is expected to rise to around 92 million

Source: World Economic Forum, Cologny, Kate Whiting, Feb 6, 2024

23%

Global jobs will change in the next five years due to industry transformation, including through artificial intelligence and other text, image, and voice processing technologies

Source: World Economic Forum, Cologny, Attilio Di Battista et al., Sept 18, 2023

Contact us:

Diana Keele
Managing Director, Cyber Security Services
dkeele@kpmg.com

Vaishanvi Nandhagopal
Director, Cyber Security Services
vnandhagopal2@KPMG.com

Ben Kramer
Sr. Associate, Cyber Security Services
benjaminkramer@KPMG.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

Learn about us: kpmg.com

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.