KPMG | SailPoint

Unmanaged Third Party Identity Risk: The Hidden Threat to your Business

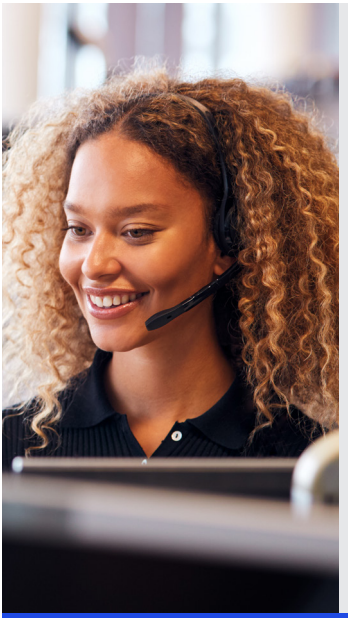
A practical guide to manage third party and non-employee identity risk

KPMG US

home.kpmg/us

The expanding identity and access management challenge

Cyber-attacks are on the rise and it's estimated as many as 60%[1] are identity based, making strong identity and access management (IAM) an increasing priority for a robust cyber defence.



48% increase in the ratio of non-employees, with one contractor being hired for every five employees[2]

90% of businesses indicate that they intend to maintain or increase their use of contractors.[2]

59% experienced a data breach caused by one of their third parties in the past 12 months.[3]

30% According to Verizon's latest data breach report – cyber breaches involving third parties has doubled from last year to 30% of all breaches.[4]

Over the past 5 years there have been dramatic changes to the way we work, digital and remote working are on the increase and with a widening digital eco system, organizations are increasingly reliant on a host of third parties who are accessing the organization's environment and this is where the vulnerability most often lies.

Whether it's business partners, contractors, consultants, freelancers, affiliates, service providers, vendors or agents – the fungible workforce has grown.

Many organizations are increasingly relying on business partners with whom they collaborate closely on strategic projects. Given the roles these partners play in the organizations, they often require some of the most privileged access to systems. This in turn introduces another layer of risk and complexity in identity management, given that it's this privilege access that is most attractive and damaging in a cyber-attack.

Through an expanding third-party footprint, the perimeter to be defended continues to grow and cyber threat actors are exploiting this. Without centralized control and consistent governance, business partner identities can become vulnerable points of entry for cyberattacks.

Crucially, getting IAM right as a first line of defence has become a critical feature of virtually every organization's cyber security posture. But a robust IAM capability must evolve and extend beyond the typical workforce to include business partners, ensuring that their access is visible, governed and regularly reviewed to reduce cyber risk.

This topic will be explored in this short guide – offering practical, effective measures, powered by technology, to better govern third party access and incorporate it into a wider identity and access management strategy.

Contents

1. Cisco Talos, 2024 Year in Review (2025)
2. Gusto, "Contractor Hiring Surges During the Pandemic. What Does It Mean for the Business Workforce?", Liz Wilke (December 15, 2021)
3. SailPoint, 2025 Gartner® Market Guide for Identity Governance and Administration (2025)
4. Verizon, "Verizon's 2025 Data Breach Investigations Report: Alarming surge in cyberattacks through third-parties" (April 23, 2025)

01

Why this matters?

Identity and access management for an organization's permanent workforce - hard enough in itself – is not sufficient to deal with the risks associated with the extended third-party and non-employee workforce.

Digital account sprawl

- On average a digital identity is estimated to have anywhere between 5 - 15 different accounts associated to it.
- The number of accounts is further proliferated for non-employees owing to the common use of duplicate or temporary accounts.
- Coupled with a lack of understanding of who is accessing them, this substantially increases the attack surface of the organization.

Over privileged access

- Given the nature of their role third parties often require elevated system access beyond standard users.
- This access is often untailored and excessive, with maximum privileges given.
- It's this access that becomes a prime target for attackers, increasing the risk of significant breaches.

More complex leaver challenge

- A core IAM control is removing access when an employee leaves.
- However, this is more challenging for third parties and contingent workers, especially when their workforce isn't fully known.
- This leads to prolonged and dormant access and increased risk of misuse.

Credential misuse

- Risk of credential exposure or misuse is increased when accounts to systems are shared.
- System complexities and teams supporting administrative tasks often lead to the use of shared credentials.
- When administrative tasks are fulfilled by non-employees, the combination of the transient nature of this workforce and shared credentials significantly increases the risk of credential exposure and misuse.

Increased attack surface

- Static privileged access is where individuals maintain high-level access for extended periods regardless of need.
- This is common for outsourced support teams who may possess administrator access even when rarely requiring it.
- This persistent access expands the attack surface and increases risk of access misuse.

02 Obtaining visibility

You cannot effectively manage what you're unaware of - so the crucial first step is gaining a clear understanding of your business's current identity position.

Questions you should ask

01 Do you truly know your digital workforce?

First, identify and profile your complete digital workforce, from permanent staff to contractors, outsourced managed service providers, consultancies, freelancers and others.

Do you have a full picture of your suppliers and third parties – what is their function in supporting the business?

02 Do you know what access your third parties have in your organization?

It is crucial to understand what access your various third parties have and to what information and systems. Access can vary considerably between different identities:

- Managed service providers and partners often have highly sensitive and privileged access to key systems in order to perform their outsourced role, making them a prime target for attacks.
- Contractors and freelancers are likely to have lower levels of access and/or privileged access to only very specific information needed to perform their role. However, these individuals rotate in and out of the organization more frequently, whilst access remains active.

03 Do you have a broader third party risk capability that can be leveraged?

Do you have a broader capability in place that continuously assesses and monitors the risks posed by vendors and partners, ensuring they meet your security and compliance standards?

It's often assumed that third parties, especially managed service providers,have their own security standards that provide adequate controls. However, almost half of leaders are only up to 50%[1] confident in the information provided and subsequently rely upon resource intensive in-house monitoring strategies. This also results in third parties needing to go through more frequent recertification.

A dynamic workforce with different identities and personas

1. Gartner Third Party Risk Management Benchmarking Report 2023

03

Taking action

Managing non-employee identities and their access to information is complex, but it isn't impossible. This should start with risk-based prioritization built on the level of access each third party has and needs.

Three foundational elements to begin to surface and manage third party and non-employee identity risk

Prioritize identifying the third parties that pose the greatest risk by taking into account:

- ☑ The role the third party plays in the organization and criticality of the services they provide.
- ☑ The volume of identities they operate on your behalf.
- ☑ The expectations of required access to systems for e.g. apps that may be under regulatory scope or critical infrastructure for important business services.
- ☑ The extent and intricacy of the information available to them.
- ☑ The turnover of staff, in particular those that have administrative or privileged access and how the joiners/movers/leavers process is managed.

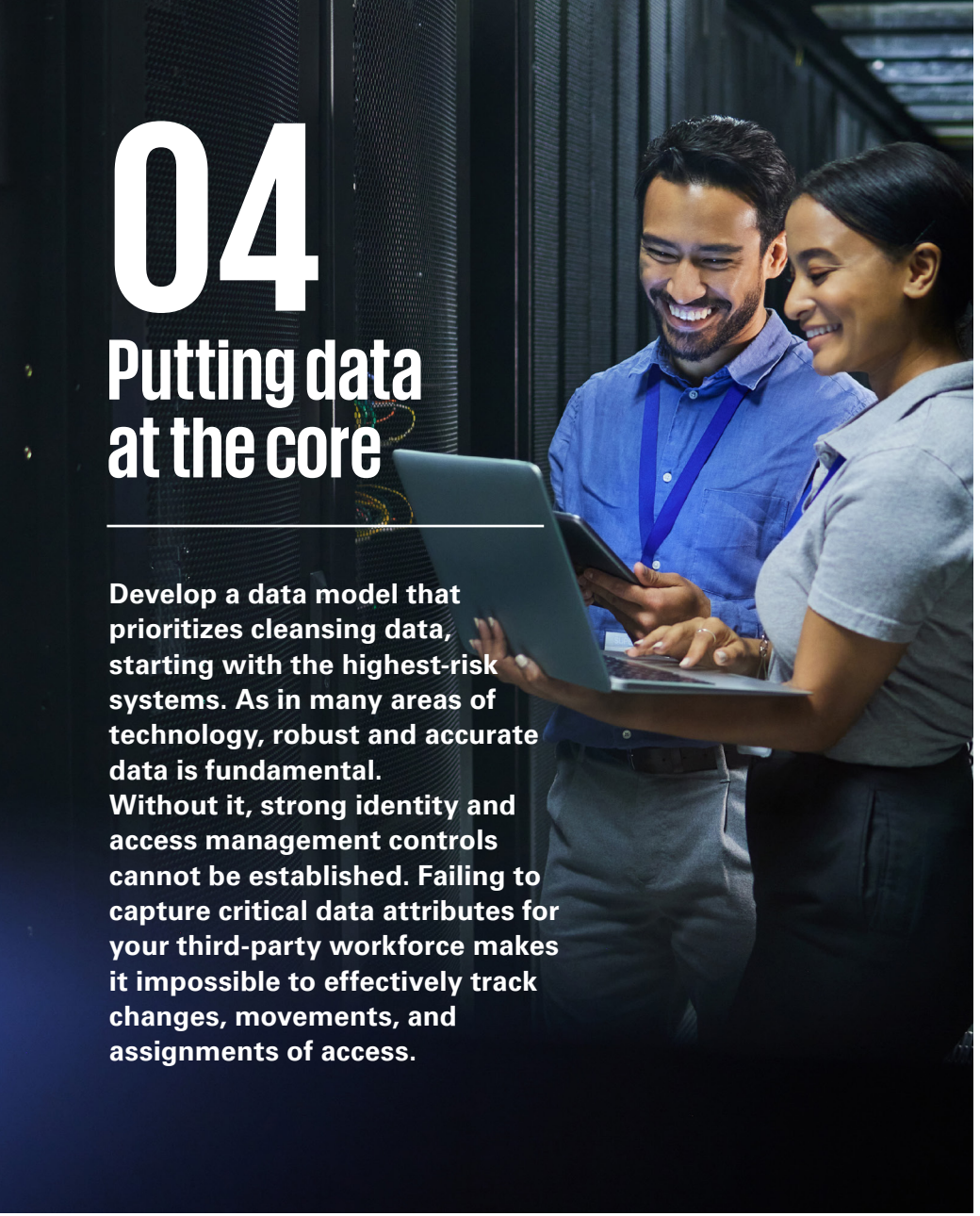
Establish a centralized, trusted source capable of integrating with existing security and identity tools by:

- ☑ Consensus on a centralized identity repository for third parties, designed to integrate with and support downstream identity tools and processes.
- ☑ Maintaining an up-to-date access repository with clearly defined data (such as who has the ability to update or modify systems) to facilitate delegated timely administration by third party representatives.
- ☑ Establishing robust access governance for both internal and external teams, ensuring comprehensive reporting capabilities that support leadership communication and compliance with regulatory reporting obligations.

Choose the appropriate technology and treat as a transformation:

Treating this as an organization wide transformation with the necessary support and selecting the appropriate technology ensures efficient deployment, long-term success and tangible business outcomes.
KPMG LLP assists organizations in evaluating solutions and business outcomes for suitability within their unique business environment.
An example of addressing unmanaged third party risk is via SailPoint's market-leading Non-Employee Risk Management tool.

- ☑ This tool provides organizations with greater transparency into their dynamic relationships with individual third-party identities.
- ☑ It enables informed, risk-based decisions regarding provisioning, verification, and deprovisioning of access.
- ☑ When properly implemented, this solution integrates with the entire IAM environment and includes automated triggers. For example, if a contractor moves to a different department, their access is automatically updated:
  - Access to their old role is revoked.
  - Access for their new role is granted.



04

Putting data at the core

Develop a data model that prioritizes cleansing data, starting with the highest-risk systems. As in many areas of technology, robust and accurate data is fundamental. Without it, strong identity and access management controls cannot be established. Failing to capture critical data attributes for your third-party workforce makes it impossible to effectively track changes, movements, and assignments of access.

Components of a data led approach to tackle third party and non-employee identity risk

Establishing a data model specifically tailored for non-employee identities that:

- Aligns with broader IAM lifecycle processes (such as leave date, the areas where they work, line management, geographic location, and other key attributes). Collecting these data points allows for the implementation of robust identity controls across the workforce and facilitates the activation of automated preventative measures where required.
- Establish these attributes as mandatory prerequisites for non-employee identity creation to ensure consistency across the workforce and embed these into your broader third party and contingent worker onboarding and vetting processes.
- Considers the varying profiles of third-party and non-employee identities, enabling tailored controls according to the specific risks associated with each identity or persona. This approach enhances control agility and targets risk mitigation more effectively. For instance, implementing robust mover controls for contractors and freelancers who frequently change roles within the organization, while focusing on regular user access reviews for service providers who typically maintain access to sensitive platforms.

Implementing data cleansing in alignment with the newly established data model which:

- Utilizes the new data model as the basis of a strategic plan to cleanse and enhance the existing digital identities and their associated accounts on an ongoing basis starting with the highest risk systems.
- Drives collaboration with application owners, partner points of contacts, and other stakeholders to methodically identify and address access issues for each application and platform.
- Remediates access by:
  - Removing unknown accounts and access.
  - Aligning access to only what is needed and to known identities.
  - Creating accountability across system owners, third party relationship owners and line managers to regularly review access.

05

Embedding non-employee IAM governance

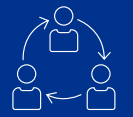
Identity and access management is an ongoing process, not a one-time update or review. It must be designed to remain sustainable, adaptable, and resilient, ensuring it can handle the continuous growth and evolution of sensitive information and managed privileges.

Success is based on strong ownership, clear accountability and effective governance

To ensure the effectiveness and longevity of IAM for the entire workforce, it must be seamlessly embedded within a broader operating model, with ownership and governance both internally and externally serving as critical components.

Stakeholder engagement and relationships development

For internal workforce IAM, key stakeholders typically include HR, IT, Security and Risk. However, based on the decentralized nature of identities, broader third party risk functions, partner relationship leads and even external agencies must all be integrated and become key stakeholders not only in the operating model but also in new processes and technology workflows.



Clarity and collaboration

Ensuring clarity is paramount, incorporate new controls into your broader TPRM and staff vetting processes. Assemble a multi-functional team to define and agree on clear roles and responsibilities, maintaining control through comprehensive visibility, while delegating administration to allow swift action when changes arise. Explore technology solutions like SailPoint's Non-Employee Risk Management tool, which can automate actions triggered by specific events and provide dynamic, end-to-end visibility of access in your environment.

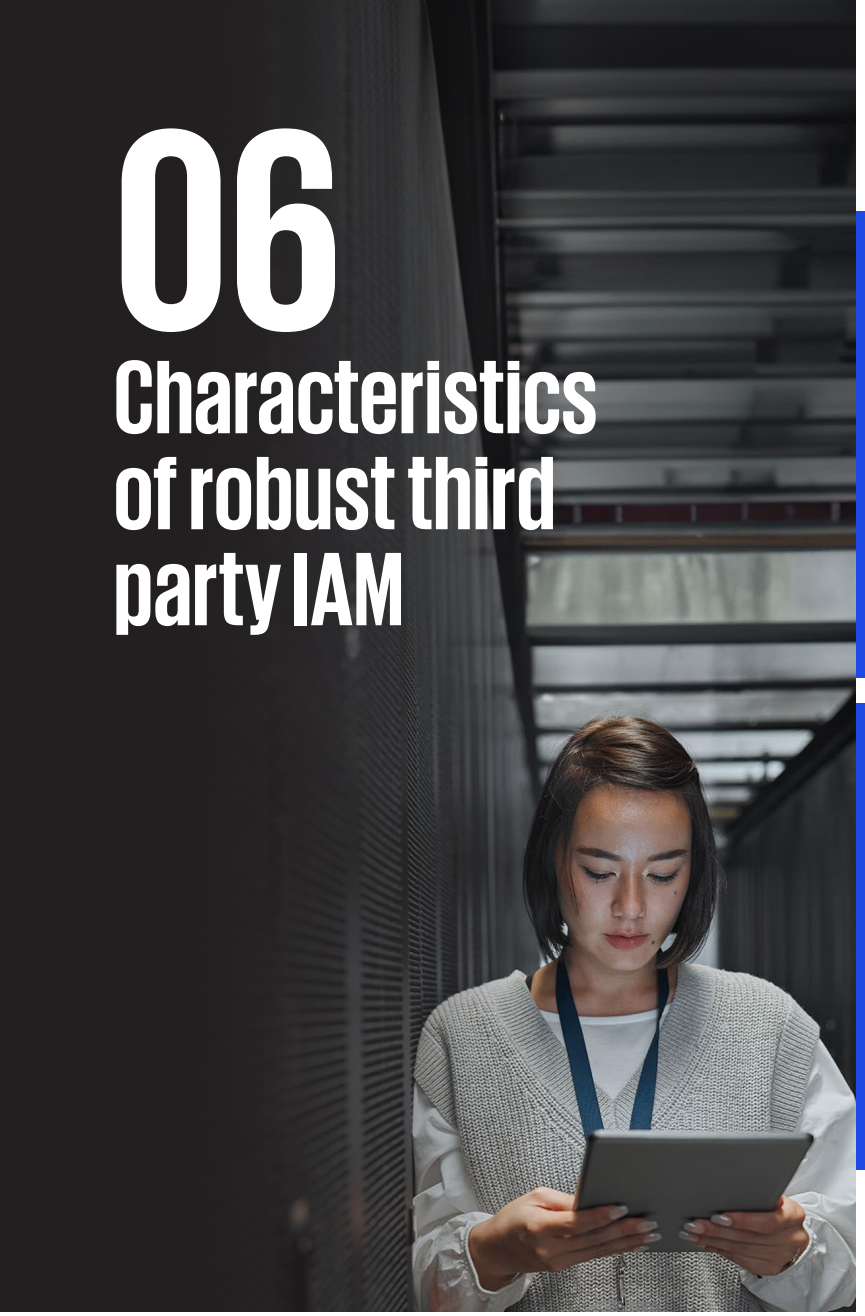
Process transformation

While technology solutions play a critical role, the real value lies in combining them with thoughtful process re-engineering and transformation. Even the most advanced technology will fall short if the supporting processes and controls are not well-designed. A strategic partner like KPMG can be instrumental in maximizing impact — guiding you through vendor and solution selection, aligning technology with your unique environment, and ensuring it drives the results you need.

Continuous improvement

Consistently review progress and analyze performance reports to ensure risks are being effectively managed. Monitor your technology environment to incorporate all systems into your identity framework. Continuously review the different identities and persona's that require access and tailor controls accordingly. Embed a culture that proactively manages identity related risk.

06 Characteristics of robust third party IAM



You have a clear, documented and verified understanding of all non-employees. There is a consistent data model to track them and they're stored centrally to feed into downstream processes.

You have identified, inventoried and tightly controlled your highest privileged and sensitive access that is used by your non-employee workforce. As a priority you've enforced multi factor authentication to access them.

You have defined roles and access rules tailored for non-employees to limit access to what's only required. This access is clearly understood and labeled, providing greater transparency of access, aiding access reviews and monitoring.

You have limited the use of shared credentials and implemented centralized credential management to store and rotate credentials used by the extended workforce, whilst also closely monitoring their usage.

You have leveraged tooling to correlate non-employee identity information with access across systems, providing a single centralized view of who has access to what across the entire workforce.

You have prioritized non-employee workforce according to levels of risk and degree of access. You've established accountability with different non-employee partners to decentralize governance of this workforce whilst integrating into your organization's broader centralized access governance processes – providing dual visibility and control.

How KPMG and SailPoint can help

Why KPMG?

Our experience

At KPMG, we have an extensive team of deep subject experts across all aspects of IAM, TPRM and wider cyber security.

Our approach

Through our proven Powered Enterprise approach, delivered through Powered Enterprise Cyber, we help organizations link cyber security with broader risk and resiliency areas. Embedding leading practices and out-of-the-box technology solutions that can be configured for optimal effect, we help reduce risk and deliver faster speed to value.

How we work with you

For IAM, we provide a full wide-ranging suite of support across the lifecycle. We can help assess your current status and desired end-state; devise a strategic approach and operating model for transformation; create a detailed roadmap with key milestones that supports you on the journey; advise on technology/vendor selection that represents the optimal fit for your business; and work side-by-side with you, through the course of the project and beyond, into post-implementation optimization and BAU.

Why SailPoint?

Our experience

SailPoint equips the modern enterprise to seamlessly manage and secure access to applications and data through the lens of identity – at speed and scale.

Our approach

As a category leader, we continuously reinvent identity security as the foundation of the secure enterprise. SailPoint delivers a unified, intelligent, extensible platform built to defend against today's dynamic, identity-centric cyber threats while enhancing productivity and efficiency.

How we work with you

SailPoint helps many of the world's most complex, sophisticated enterprises create a secure technology ecosystem that fuels business transformation.

Better together

KPMG is a leading implementation alliance partner of SailPoint solutions with a focus on achieving business goals through technology enablement.

As a SailPoint Delivery Admiral in 2021, 2022, 2023, and 2024, KPMG has delivered some of the largest global deployments.

Together, we tackle and accelerate the delivery of highly complex IAM programs ultimately meeting our client's business needs today and preparing them for the future, saving time and money, and advancing long-term ROI.

If you're ready to take the next step and believe we can assist, please don't hesitate to reach out. To learn more about KPMG, our alliance with SailPoint, and the work we do, there are several resources available to deepen your understanding.

You can read more about KPMG Powered and our Cyber Security Services **here**.

You can learn about the KPMG and SailPoint alliance **here**.

More detail on KPMG and our full range of capabilities and services can be found **here**.

KPMG was named as a SailPoint Delivery Admiral in 2021, 2022, 2023, and 2024 in recognition of our commitment to accelerating innovation and enhancing our clients' cyber security experience.

Please speak to our SailPoint and Cyber Security/IAM specialists:

Hemal Shah
Partner
KPMG US
hpshah@kpmg.com

Mike Hatjiyannis
Managing Director
KPMG US
mhatjiyannis@kpmg.com

Adam White
Managing Director
KPMG US
hpshah@kpmg.com

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

Learn about us: **kpmg.com**

Create: CRT159407E