The identity gap in third party risk management

To increase flexibility and boost competitiveness, organizations have eagerly embraced growing and diverse populations of consultants, partners, vendors, and other contingent labor, as well as non-human technologies like service accounts, bots, and smart devices. While these efforts are intended to fortify competitive strategies, many organizations are now realizing that by leveraging these third parties they also create new operational challenges and expand their attack surface, dramatically increasing their cyber risk exposure. A leading challenge is managing the secure access of these third-party identities.

The strategic opportunity: Organizations of all sizes have the unprecedented opportunity to innovate, grow faster, improve profitability, and ultimately create greater customer value by utilizing a variety of resources beyond their traditional employee base. Oftentimes, these resources are available on demand, have unique or underrepresented skillsets, and do not require the same long-term monetary investment as full-time employees.

The drawback: Most organizations have no centralized, cohesive way to track and manage their relationships with this burgeoning number of third-party users, or “non-employees”. This is most critical when it comes to authorizing the legitimate, appropriate access to organizational assets (facilities, systems, and data). Many organizations have unsuccessfully attempted to solve the problem by customizing their existing human resources information system (HRIS). Others have tried to build their own proprietary systems, or cobble together a solution from disparate applications. While these systems may address some operational challenges, none are designed to mitigate the risk these non-employees create as unmanaged, unsecured outsiders with insider access.
Who are third party users?

A third-party user is any resource with access to facilities, systems, or information who is not an employee of the organization that granted that access. In today’s extended, integrated business environment this includes a wide range of workers from different sources such as: staff from a temporary agency, consultants, contractors, cloud or hybrid software vendor personnel, on-premise software support, supply-chain workers, other professional services or service provider personnel.

But third-party vendors are just one category of non-employee users. Other types include project-based or Statement-of-Work (SOW) workers, customers, students or interns, and volunteers. For organizations built on the franchise model, franchisees might fall under third-party, non-employee users.

Increasingly significant in a more digital world, third-party access is also granted to non-person entities, including service accounts, bots, robotic process automation (RPA), IoT devices, and operational technology (OT) controls. These are particularly prevalent within the manufacturing industry and for organizations with sizeable supply chains.

While each of these organizations and non-employee groups have their own distinct characteristics, the concerns – and challenges – of providing access to any of these resources are fundamentally the same.

Identity governance for employees vs. third-party users

Identity governance for employees is much more manageable than governance of third-party users. Put simply, the organization has much more direct and complete control over employees’ identity and access.

Managed fully by a single department (Human Resources or People Operations), the identity lifecycle of an employee is typically an orderly progression of managed, tracked, and documented activity, from the opening of a position, the selection of candidates, the offer, screening and onboarding activities, job promotions or transfers, and termination. At each stage the organization authorizes and manages the appropriate access. While other departments may be involved, a single team is accountable for communication, progression, and meeting corporate security and compliance requirements. For example, HR technologies typically integrate with downstream technologies such as IT Ticketing, which can kick off and track workflows.
The identity governance, most importantly, the authorizing of the appropriate access of non-employee users, is far more chaotic and less linear. For starters, even large enterprises often lack formal procurement vetting and identity management processes for third parties. These responsibilities are often distributed across lines of business, including legal, HR, compliance, and information security. A third-party relationship also needs to be coordinated by resources within (sponsors) and outside (delegates) of the organization. Current disconnects in this process and lack of transparency into non-employee identities heighten the risks of inappropriate access, for example, over-provisioned and orphaned accounts.

“Many organizations have strategic shortfalls in third-party risk management governance. Specifically, only 42 percent of respondents say managing outsourced relationship risk is a priority in our organization and only 40 percent of respondents say there are enough resources to manage these relationships.

Gauging third-party identity security maturity

Organizations often have trouble gauging their level of maturity in managing third-party identities. The actual challenges and risks can be vague (and unrecognized) because the operational activities are distributed across teams. In our experience working with clients looking for the answers to the following key questions allows them to begin to gain more clarity:

- How many vendors do you have?
- How many third-party users do you have?
- How much does it cost us providing and managing the lifecycle of third-party access?
“How many vendors do you have?”

Due to a lack of a robust centralized system and processes most organizations still struggle to understand how many vendors – and associated identities – they are providing access to. It is not unusual for an organization’s guessed answer to be only a fraction of the true number discovered upon actual research.

The number of third-party vendor relationships naturally varies depending upon the type and size of organization. Though it is difficult to get specific numbers, many organizations have hundreds of third-party vendor relationships. If your organization is multi-national, or in certain sectors like manufacturing or retail, the number could be in the thousands. This trend is accelerating in the digital economy, with service providers for virtually every facet of running a business: from payroll to cloud provisioning.

It is important to note, these relationships are not static. Organizations continually adapt and change their vendor relationships. The number of individual third-party identities associated with each of these vendors can scale and complicate your operational challenges exponentially.

“How many third-party users do you have?”

After determining your total number of vendors, the next question is: How many users from those organizations have been provided access to your facilities, systems, and information? Often this too is another mystery. Each vendor company may have hundreds or thousands of users. This number is higher for certain industries such as healthcare, manufacturing, and education, where a ratio of one employee to multiple non-employees is common. And bear in mind, third parties themselves are dynamic. Vendors are also hiring and reducing employees (and their third-party non-employees!) based on their changing business requirements.

With utilization of third parties continuing to increase, it may become more common for over half of an average organization’s workforce to be non-employee users. This projection doesn’t even take into consideration a slew of other non-employee identities that are not vendor employees: students/interns, SOW employees, freelancers, and volunteers. Nor does this account for the challenges introduced by the increasing number of non-human identities that require access.
The identity gap in third party risk management

“How much does providing this access cost?”

Food for thought. When an organization is considering the cost of a new contract, it rarely considers the full expense required to onboard, manage, and terminate access for related third-party users. This is just one example of the unaccounted-for organizational cost provisioning and managing third-party access.

One SailPoint Non-Employee Risk Management client recently investigated the effort to onboard third-party users using existing tools and processes. Totaling the time spent by lines of business and an HR resource they found they invested up to 40 staff hours per non-employee identity, and this organization applied a simple red light/green light access strategy. While this estimate includes the steps for authorizing physical and logical access, it doesn’t include the additional time needed to validate active engagement status, manage access changes, audit for compliance needs, and terminate access.

Clearly, organizations need to improve efficiency – and visibility – going forward. They also need to better manage security and financial risks by matching security controls to the vendor and individual user risk profiles. This approach also empowers your employees typically involved in non-employee onboarding, monitoring, and (hopefully) offboarding, to focus on higher value tasks.
Breach risk: the wildcard hidden expense

The risk of a cyber breach is the most public and overtly negative outcome from improperly or unmanaged non-employee user access. Below are several all-too-common procedural scenarios that can lead to an increased risk of a breach.

<table>
<thead>
<tr>
<th>Risk</th>
<th>Scenarios</th>
</tr>
</thead>
</table>
| A potentially disgruntled user is not prevented from reentering the organization | A former employee who appears on the Not Eligible for Rehire list subsequently joins a vendor team and receives access to the organization’s resources without being checked against that list.  
  A former consultant who left the organization on poor terms changes names before being hired through another consulting team. |
| The vendor relationship is orphaned due to turnover                  | A business line leader who manages vendor resources exits the organization, leaving a gap in sponsorship for the third party.  
  A vendor’s client manager leaves without providing the organization with contact information for his or her successor. |
| Access is not terminated on a timely basis                           | A user terminates employment with a vendor company without the organization’s knowledge, or moves on to work with other clients, and access remains authorized.  
  A hacker breaches unattended third-party credentials, perhaps through a password reuse attack, resulting in a breach. |
| Too much access is granted                                          | The organization has over-provisioned or provided access in excess of the users needs, potentially putting regulated or confidential information at risk of accidental access.  
  Access is granted based on manual requests without proper identity context to validate that requested access is appropriately limited.  
  Non-employee users have excess access that attackers can leverage to acquire higher levels of privilege. |
| Outsiders made insiders                                             | The organization has taken outsiders, third parties, a category acknowledged by security professionals to be high risk and provided them with generous insider access, compounding their risk exposure. |
Emerging compliance risks

Regulation of data security and privacy continues to evolve worldwide. And given the escalating frequency and scale of cyber breaches, it is very likely increasing regulation will remain part of running a business.

Managing and securing identities to enforce separation of duties (SoD) has been a part of financial regulations such as Sarbanes-Oxley (SOX) and Graham-Leach-Bliley (GLB) for some time. The European Union’s General Data Protection Regulation (GDPR) contains several mandates reliant upon timely and accurate identity and access management. These include the protection of an individual’s data (including identity data) from unauthorized and unlawful processing, accidental loss, destruction, and damage. This data protection must be implemented “by design and default.” Another is the Right to Erasure, known as the Right to Be Forgotten. The Right to Be Forgotten has been adopted by a number of other regulations, most notably the California Consumer Protection Act (CCPA), which came into effect in 2021. Both GDPR and CCPA come with heavy fines for non-compliance.

One example of the challenges. It is common for an organization to move the accounts of terminated users to a special Active Directory organizational unit for terminated users instead of deleting the accounts. Only through a master identity record can an organization identify the user’s geographic location to determine which laws apply and fully delete the user’s history of access as requested.

These regulations are just the tip of the iceberg regarding identity and securing access. Many more highly regulated sectors face even more stringent industry-specific compliance requirements: healthcare (HIPAA, HITECH), manufacturing (OSHA, DOT) and financial services (FINRA, SEC).

Until organizations implement comprehensive and centralized identity and access systems that can cover third-party, non-employee users the risk to compliance will only increase.

Signs your approach to third party identity management is failing

Your third-party non-employee identity management efforts are ineffective if the organization:

- Doesn’t have an accurate count of vendors or associated non-employee users, or a clear understanding of the information those entities can access or are collecting.
- Doesn’t immediately cancel access upon termination of a third-party user.
- Manages onboarding/provisioning and termination/de-provisioning for third parties with undefined, manual process(es).
- Views the risk of non-employees as comparable to employees but applies a
The identity gap in third party risk management

Fraction of the rigor used for employees.

• Can’t recognize a former employee or third-party user who returns to the organization in another role.
• Uses a green light/red light approach to risk rather than implementing risk levels with appropriate security controls designed for each level and type of user.
• Lacks the ability to evaluate or rate risk at the individual identity level.
• Treats third-party identity management as a distributed function, rather than the clear responsibility of one unit or group.
• Approves privileged access without requiring approval of an exception or acceptance of risk.
• Views third-party identity management as a business risk that is too hard to tackle so should be addressed with mitigating controls.
• Decouples identity management from third-party risk management.
• Believes that the responsibility for onboarding and non-employees belongs solely to HR and so does not automate collaboration between needed internal and external stakeholders.
• Can’t automate compliance audits and requires expensive, time-consuming manual efforts.
• Tries to manage non-employee identities either by customizing an existing HR, building a proprietary system, or putting together ad hoc process and existing systems.

Signs of successful third-party management

• Your third-party user and identity management efforts are likely to be far more effective if the organization:
  • Makes informed access decisions using a central repository of all third-party users that contains details about their relationship to the organization such as: the vendor they work for, the vendor’s delegated admin, the vendor’s internal sponsor, etc.
  • Immediately cancels access upon termination of a non-employee user or the vendor they work for.
  • Easily identifies former employees or non-employee users who return to the organization in other roles.
  • Acknowledges that non-employees pose a higher risk level than employees and should be treated with more rigor, not less.
  • Assigns a risk rating to individual third-party users (and not just the vendor), taking into account risk inherited from the vendor they work for, location, credentials, access level, and other factors defined by the organization.
  • Treats personnel from a high-risk company as high-risk users.
  • Allows an organization to truly manage the identity lifecycle rather than just managing current access.
  • Manages onboarding/provisioning and termination/de-provisioning for non-employees using well-defined, risk-aware, automated process(es).
• Automates compliance audits with minimal manual intervention.
• Requires exception approval or risk acceptance to be approved before allowing privileged access.
• Uses efficient systems and processes to manage human and non-human identities to automate legacy, manual, time-consuming, and costly processes.
• Prioritizes third-party identity management as an organizational need that can’t be effectively contained through mitigating controls.
• Tightly couples identity management and third-party risk management.
• Manages non-employee identities through automated collaboration between responsible internal and external parties, including the third-party user.

The SailPoint Non-Employee Risk Management approach

SailPoint can help. Our Non-Employee Risk Management solution provides a comprehensive set of capabilities that help organizations improve operational efficiency and reduce the cost and risk of managing third-party identities. Because third parties are widely acknowledged by security professionals as high risk, SailPoint gives special consideration to the risk related to the individual, non-employee’s identity when providing insider access to facilities, systems, and data. With SailPoint, organizations have better transparency into their dynamic relationships with each individual third-party identity and are thus able to make well-informed, risk-based decisions about provisioning, verifying, and deprovisioning access.

The Non-Employee Risk Management solution addresses the limitations that have long prevailed in homegrown, HR, ad hoc solutions. and uniquely offers:

• A purpose-built, authoritative source of identity and access data for non-employees
• User-configurable portals that enable organizations to drive collaborative and continuous non-employee data collection from both internal and external resources.
• A hybrid solution for identity and third-party risk management.
• Specialized use case support for industries, M&A, and non-employee types ranging from volunteers, students, independent contractors, freelancers, partners and non-humans like bots, service accounts, and IoT devices.
• Dynamic relationship management for organizations to capture the multi-dimensional relationships they often have with non-employees.
• Risk ratings at the individual identity level.
Conclusion

While third-party resources can provide today’s organization with many benefits, managing their identities and access needs present new operational and security challenges. Attempting to address with HRIS, proprietary, or overly labor-intensive, manual processes that are prone to error increase the costs and risks to the organization. The result is not only operational inefficiency and high cost, but a fertile hunting ground for hackers.

Moving forward, what is required is a true third-party identity management solution that turns chaos into order by increasing efficiency, eliminating over-provisioning and untimely de-provisioning, and reducing risk. With a purpose-built system for non-employee identity management, organizations have more transparency and control over their non-employee populations and as a result can lower labor-related costs and make well-informed, risk-based decisions about access, ultimately reducing the risk of a third-party breach.