Non-employee identity security and lifecycle management

The business significance of third parties

Organizations are managing an increasing number of third-party, non-employee identities: partners, vendors, seasonal workers, affiliates, consultants, contractors, agents, and service providers.

Business leaders continue to leverage a non-employee workforce. In 2019, 60% of organizations were working with more than 1,000 third parties. And looking just at the hiring of contractors: The ratio of non-employees to employees has increased by 48% since 2017; one non-employee is now hired for every five employees. This trend shows no signs of slowing down, with 90% of businesses indicating they intend to maintain or increase their use of contractors.

“Businesses view contractors as essential to their success. Over 62% of businesses surveyed said either that their company’s success was dependent on contractors or it would be much harder to have a profitable business without contractors.”

From the MPF. Source: Contractor Hiring Surges During the Pandemic. What Does It Mean for the Business Workforce?
Many businesses also enable non-humans to extend their workforce, including service accounts, RPAs, devices, and bots. In our recent “The Horizons of Identity” research report – where we surveyed over 300 global cybersecurity executives for their insights – we found that machine identities make up 43% of all identities for the average enterprise, and are among the top two identity categories to grow the fastest over the next 3 – 5 years. On top of that, the total number of identities is projected to grow by 14% over the same span.

Non-employees and non-humans can have a variety of relationships with an organization. Yet – just like employees – their access to an organization’s internal systems and data needs to be authorized, attested to, managed, and tracked appropriately. In order to secure the enterprise, more than ever it is vital to understand and define precisely who these non-employee/third parties are:

- To collect the necessary identifiers.
- To determine exactly what their relationship is to the organization.
- To establish what business role they will fulfill.
- And critically, who is responsible for their relationship.

**Contractor-to-Employee ratio has increased 48% in 5 years**

From the MPF. Source: Contractor Hiring Surges During the Pandemic. What Does It Mean for the Business Workforce?
One of the greatest risks facing organizations today is the lack of controls and auditable processes associated with securing a non-employee identity lifecycle. A great example is the simple on-boarding, attestation, authorizing appropriate access, and importantly, off-boarding of third parties in a thorough and timely manner:

Growing risks to the business

The reality is a large majority of cyber security breaches today occur as a result of non-employee identities. According to Ponemon research, 59 percent of respondents confirm that their organizations have experienced a data breach caused by one of their third parties and 54 percent of these respondents say it was as recent as the past 12 months.

Has your organization ever and in the past 12 months experienced a data breach or cyber attack caused by a third party?

- Experienced a data breach caused by one of the third parties: 59%
- Experienced a data breach caused by a breach of one of the third parties in the past 12 months: 54%
- Experienced a data breach caused by a breach of one of the Nth parties: 38%

From the MPF. Source: Contractor Hiring Surges During the Pandemic. What Does It Mean for the Business Workforce?
The third-party identity breach that really caught the public’s attention was the Target breach of 2013: 40 million credit and debit records and 70 million customer records, a $18.5m settlement – not including operational and brand costs. Unfortunately, the vulnerabilities still exist, and have arguably gotten worse. Just a sampling of 2022 third-party attacks include:

- Major Car Manufacturer exposes data on 300,000 customers; result of a mistake by a website development contractor;
- Leading ride-sharing organization suffered a data breach after a threat actor leaked employee email addresses, corporate reports, and IT asset information stolen from their third-party vendor mobile device management platforms (MDM) service provider.
- In US Healthcare, 1.91M healthcare records were compromised by breaching a debt collections company. 3.65M patient records were exposed via a provider of electronic health records to eye care providers.

The trend for attacking business associates (third party services) is clear:

![Data breaches at HIPPA-Regulated entities](image)

Of a recent survey of over 1,100 IT and IT security professionals familiar with their organization’s approach to managing risk, 60% stated the number of cybersecurity incidents involving third parties is increasing.

While companies are increasing their reliance on third-party entities, not just contractors, but vendors, affiliates, consultants, service providers, service accounts, bots, etc., cyber-criminals are becoming more adept and sophisticated at identifying and attacking these expanding vulnerabilities. Businesses need the flexibility and cost-efficiencies of cloud computing and distributed applications: just think of digital transformation. Yet
organizations of all types need to take a serious look at how they manage the identities and access for these third-party non-employees.

Challenges for existing systems and processes

For many organizations today, there is no system in place that is inherently designed to manage the dynamic and increasingly complex relationships between a company and these non-employee, third parties. Organizations may depend on manual, home grown, disparate, or customized systems and workflows which were never meant to handle the volume or complexity of today’s third-party relationships.

Ad Hoc or Custom Builds: These solutions range from the simple — for example managed directly in Active Directory, or an Excel spreadsheet where non-employee contact data is kept— to the overly complex: a custom-built application (or multiple apps cobbled together) that’s absent of a mechanism for external registration, features code heavy UI, and isn’t built for easy audits and changing compliance requirement.

Human Resources Information Systems (HRIS): However tempting, it is not practical nor cost-effective to use a HRIS to create an authoritative source of identity security and management for non-employee users. These systems are designed for employees, not third parties, who are fundamentally different. Third-party, non-employees have unique, non-linear relationships with the organization, frequently require collaborative onboarding and identity lifecycle management outside the organization. And storing non-employee data in HRIS may create legal liability for the organization, specifically employee tax and benefit implications. In certain jurisdictions housing non-employee data in your HRIS is simply illegal.

Vendor Management Systems (VMS) Quite simply, VMS approaches are not rooted in identity security. They don’t account for the increasing risk to the business specific to securing third-party identities. For example, they may not make it easy to collect and house relationship details (i.e., engagement time frames, which specific projects, etc.) that are relevant to security risk and compliance.

Factors that contribute to third-party identity security issues:

- **Management and oversight** of non-employee, third parties is slow, inefficient, and ineffective.
- A comprehensive **identity** repository for third parties doesn’t exist at all.
- Defining the **complex relationships** and even identifying who should own – and be responsible for – these identities is lacking.
- Growth in the **blended workforce** has made the identity lifecycle more difficult to manage.
- **Poor identity management** leads to poor access management.
Digital transformation drives demand for an increase in third-party access to sensitive data.

Not only are non-employees and non-humans now a greater part of the workforce, but third-party relationships also change on a constant basis. It’s not uncommon for an employee to become a non-employee and then potentially make the move back to employee later, or for a non-employee working for one vendor organization to transition to another vendor organization.

These use cases merely scratch the surface of the level of complexity, and the increasing risks to the business, that exists when dealing with securing the third-party identity lifecycle.

Knowing the difference between identity and access

It’s not uncommon to hear someone, even in the IAM industry, say the word “identity” and immediately start talking about access. The two are not synonymous. An identity is who the person is, what their business role is, and what their relationship is with an organization. Access defines what corporate applications and data are authorized for use by a specific identity. Inextricably linked, but not the same. This may be why so many incorrectly believe that an identity is what a person can access.

Several other Identity Governance and Administration (IGA) systems claim to “enable the right individuals to access the right resources at the right times for the right reasons.” In reality, these systems depend on other sources to determine who the “right individuals” are and fall short when attempting to manage non-employee data, their changing relationships, and appropriately managing access. When a comprehensive source of people data does not exist, other IGA systems fall short in their promise to effectively manage access to non-employees. This leads to a high rate of ineffective identity programs and increased risk to an organization.

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.
Reasons why the identity problem is worse than ever:

- Businesses assume an account in a system is an identity when it is not.
- Peoples’ relationships with an organization, particularly third-party, non-employee relationships, change over time.
- Businesses have little to no governance on their service accounts.
- The end of one relationship with an organization may be the beginning of another relationship within the same organization, or extended ecosystem: think vendors or supply chain resources.
- A growing part of the enterprise workforce is comprised of non-employees and non-humans.
- Outside of HR, management and oversight – and prioritization – of identities is poorly addressed.
- Multiple authoritative sources often exist which are not handled well by IGA systems.
- Identities are increasing exponentially, particularly with the use of third-party cloud service (each of whom have unique identity paradigms).

The fact is that HRIS or VMS systems are not enough, and certainly not fast enough, to handle the complexity and dynamic nature of securing third-party identities. Other IGA systems also have challenges, specifically when it comes to securing the expanding and dynamic environment of third-party access. And, let’s face it, by and large they were not designed to do so.

Yet, the risk in not managing all identities properly is high: from cyber compromise resulting in ransomware or theft of valuable corporate information, to operational inefficiencies, audit issues and non-compliance.

Preventing a breach or compliance issue via a third-party requires systematically tracking all individuals with access to business systems and data. Only by putting identity first and then correlating appropriate access will an organization be able to ensure a secure identity perimeter that incorporates non-employee third parties.

The non-employee relationship challenge

Non-employees have relationships to other identity types, such as contractors to contracts and contracts to vendors. Management of these identity types are often managed by different departments within the organization. It is not uncommon to have some of these relationships managed by separate processes or workflows with no collaboration.

When contractors are onboarded and access is created in the various corporate systems, there is nothing that ties that contractor to a contract or the contract end date to the contractor’s end date. Therefore, when a contract ends, there is no way to trigger the business process for terminating contractors tied to that contract.
Furthermore, an identity can have multiple relationships with an organization. However, as it currently stands, most organizations base a relationship type off a single attribute. For example, someone may start off as a contractor and then move into a full-time employee role. Or a student at a college may graduate and subsequently gain employment at their alma mater, moving them from a student identity to a staff identity.

Companies need a more flexible, rapid way to manage all identity types and the relationships they can and do have within an extended ecosystem.

Who is responsible for the non-employee identity?

Employee and non-employee access is ultimately the responsibility of IT security, while employee identities are (hopefully!) the responsibility of human resources. But who is managing third-party, non-employee identities?

The short answer is often no one.

Why isn’t procurement or human resources responsible for managing relationships between organizations?

Procurement
Procurement manages relationships between organizations which can include sourcing and contracting potential vendor partners. Vendor management systems (VMS) are ill suited for storing people data and their associated relationships with an organization. Much like an HR system, merely attempting to manage these people in a VMS system would result in heavy customizations, static processes and ultimately prove to be cost prohibitive. Procurement departments are uninterested and unequipped to manage individual relationships.

Human Resources
Human Resources is the expert on employee relationships. The typical HR system covers some Identity relationships but struggles to manage multiple identity relationships, something that is not easily accomplished and is cost prohibitive in an HR system. Ultimately, the HR department’s primary focus isn’t to provide identities to an IGA system, but to focus on managing, recruiting and hiring employees, coordinating employee benefits and suggesting employee training and development. HR knows the data and processes required to manage employees (or a sub-set of them).

Challenges human resources must overcome:

- HR resource constraints
- Cost prohibitive licensing
- Heavy customization to manage business process
- Limited ability to manage varying types of identities and relationships
- Incremental total cost of ownership over time
Identity workflows will continue to diversify

The ‘one-size fits all’ approach to identity management is doomed to fail. Unfortunately, using IGA tools that haven’t evolved, or trying to extend HRIS or VMS systems to create and maintain varied third-party identity workflow processes is costly, time-consuming, and will not meet company needs.

An effective solution would provide a simple, cost-effective tool that enables configurable workflow processes for a complete non-employee lifecycle, even for different third-party populations (including non-humans) with unique requirements. Given that capability, there is no need to settle for risky, error-prone manual processes, patched together by different groups lacking any centralized control or accountability.

Organizations must also recognize how important collaboration between integral departments, namely human resources, information security and the overall business, is to their ultimate success. The identity solution must provide the ability to view, identify, and track a non-employee or non-human’s relationship with your organization to better determine why its identity requires access.

The end result: an effective third party, non-employee identity management system of record for identity and access that allows companies to gain greater control over their risk and empower the extended network and velocity with which they need to conduct business.

IT Compliance Benchmark Survey

Many organizations have become keenly aware that they need to get better at managing IT risks arising from the use of third-parties.

Three-quarters of all surveyed organizations said they have a process in place today to identify, treat and monitor third-party risks — but their processes aren’t working well.

51% plan to expand their third-party risk management program.

90% of all survey respondents reported being negatively affected by a third-party incident in the past year.

Solving the identity problem

Securing your businesses requires an intelligent identity authority that informs you “who” someone is, “why” they require access, and “when” access is appropriate. Any third-party, non-employee identity program must be built on a comprehensive identity lifecycle management platform — one that can capture and manage the full spectrum of identities and their associated relationship(s) to drive the appropriate, secure access to valuable data and applications.

Companies must start with defining the business requirements around the various identities, the lifecycle of those identities and the relationship to the organization. An effective solution for third-party identity management should enable the responsible identity owners, those who know the required data and processes, to manage their section of the identity population while feeding a central identity authority. Delegated administration and more automated identity processes are more efficient and accelerate the time to value for your extended enterprise.

The solution should allow companies to strengthen security with identity-based risk scoring. Scoring enables organizations to execute risk-based identity and access lifecycle strategies to better secure their third-party ecosystem. And more automated individual or large-scale identity verification processes integrated into the lifecycle process reduces risk and helps to mitigate third-party breaches.

Having a single authoritative source for identity and access as well as intelligent third-party identity lifecycle management allows organizations to:

- Better manage risk with identity verification and risk scoring.
- Account for and manage all identities based on a defined relationships.
- Improve governance and administration of access with better visibility across non-employee and non-human identities and access.
- Gain efficiencies by eliminating wasteful, time-consuming processes.
- Streamline and automate business processes to collect and maintain identity information more collaboratively and efficiently.
- Enhance user experience with delegated administration and more self-service options.
- Achieve audit and compliance easier and faster for all third-party, non-employee identities.
An intelligent identity solution should

**Allow identity defined business processes**
The ability to have different processes based on the identity type is paramount in effectively managing a variety of non-employee identities. For example, in healthcare the onboarding process for a clinical provider is very different than that of an IT contractor, etc.

**Enable the business to manage identities**
The business needs secure, user-friendly tools to safely allow managers, outside vendors, sponsors, and the non-employee themselves, to manage their piece of identity data.

**Support flexible and easy to configure workflows**
Allow for configurable and collaborative identity process that includes basic functionality such as, document attachments, custom attributes, varied approval and review steps, collaboration, and notifications.

**Maintain a single identity despite changing relationships**
A person’s relationship with an organization is not always static. Third-party, non-employees may change their relationship with the organization, e.g., as in the case of service providers, vendors, or healthcare workers.
Check out the SailPoint Non-Employee Risk Management solution

With the SailPoint Non-Employee Risk Management solution, organizations can easily collect third-party, non-employee data in a collaborative and continuous manner, both from internal and external resources, throughout the lifecycle of the non-employee. Because its purpose-built, the solution can manage the complex relationships organizations have with their entire extended enterprise in a single, easy-to-use application that simultaneously helps facilitate commercial initiatives, supports regulatory compliance, and reduces third-party risk.