MANUAL APPROACH TO MANAGING NON-EMPLOYEE AND NON-HUMAN IDENTITIES LEADS TO SECURITY ISSUES

A Global Survey of Security & IT Professionals and Executives

July 2023

dimensional research

Sponsored by SailPoint

MANUAL APPROACH TO MANAGING NON-EMPLOYEE AND NON-HUMAN IDENTITIES LEADS TO SECURITY ISSUES

A Global Survey of Security & IT Professionals and Executives

Dimensional Research | July 2023

Introduction

This paper reviews key findings from a global research survey across 339 participants to understand how companies manage non-employee and non-human identities and respective access privileges. The research compared those approaches, processes, and corresponding workload efforts to that of managing employee identities. The survey then focused on the occurrence and ramifications of granting inappropriate access or failure to remove access when the work was completed.

Executive Summary

97% of companies provide access to non-employees and nearly 9 in 10 provide access privileges to non-humans. However, 54% of executives surveyed revealed that inappropriate access granted to a non-employee or non-human has resulted in severe security issues such as loss of control of resources, data loss, compromised intellectual property, direct security breaches, and more.

51% shared inappropriate access had been provided to non-employees and 16% reported they don't know, which is actually more concerning. The research finds that granting access to non-employees is difficult, with more manual steps than with employees, and requires actions and approvals from numerous employees. Removing access is just as laborious with 83% requiring manual tasks to remove access. This high effort in managing non-employees has resulted in a practice of just disabling identities. Only 1 out of 3 companies fully delete an identity and its related access when the working relationship ends.

Just 51% of companies know in real-time which non-humans are accessing their system. Half of the participants admit they have granted inappropriate access to non-humans and 14% again don't even know. Following the trends from non-employees, granting access requires several employees and numerous manual steps. This again leads to only 42% of companies fully deleting non-human identities and related access privileges when access is no longer needed.

Participants provided a multitude of different processes and policies for managing non-employees and non-humans, but the lack of consistency indicates immaturity in methodology, best practices, and tools. This immaturity has resulted in nearly 7 out of 10 companies stating they have an issue with duplicate and orphaned identities. Simply put, the predominately manual approach to managing non-employee and non-human identities and access is impacting business with short term and long term security issues, and compliance risk, while wasting IT and security resources. Companies need to find a better, automated solution to managing the cyber keys to the business.

Key Findings

- Critical Security Issues Result from Providing Inappropriate Access to Non-Employees and Non-Humans
  - 97% of companies provide access to non-employees
  - 88% of companies provide access privileges to non-humans
  - 54% of executives share that non-employees or non-humans with inappropriate access rights have resulted in a security issue
  - 86% state inappropriate access has result in loss of control of resources, data, intellectual property, and more

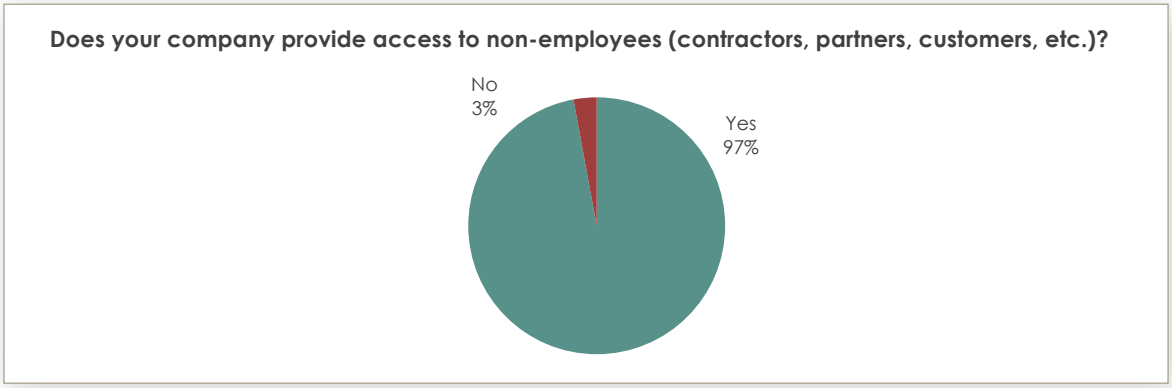
- Manual Processes Lead to Unknown and Inappropriate Access Privileges and Failure to Remove Them
  - 51% admit inappropriate access has been assigned to a non-employee, 16% didn't know if they had
  - 55% shared they have realized access was not removed after a non-employee working relationship ended
  - 83% require a manual process to remove access from a non-employee when the working relationship ends

- Most Don't Know which Bots, Applications, or Services have Access to their Systems
  - Barely half (51%) of companies know at any point which non-human identities are accessing their systems
  - 50% of companies admit their company provided inappropriate access to non-humans, 14% don't know if they had
  - Only 42% fully delete identities and related access privileges when non-human access is no longer needed

Detailed Findings

Non-Employees Have Access to Applications and Data

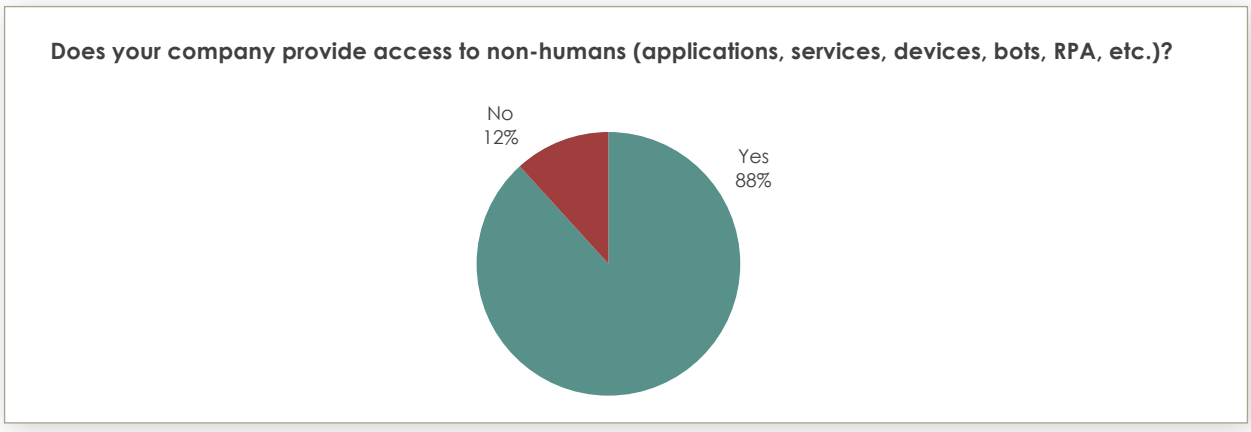
This research confirms a business trend that companies unilaterally rely on contractors and partners to operate their businesses. In order to enable those non-employees access to resources, access is commonly granted to key applications and related data. In addition, many companies provide access to their customers. For many industries such as banking, manufacturing, retail, or shipping, this access is necessary to support their supply chain effectiveness. The bottom-line is 97% of companies provide access to their applications and data to non-employees.



Non-Humans Have Access to Systems and Data

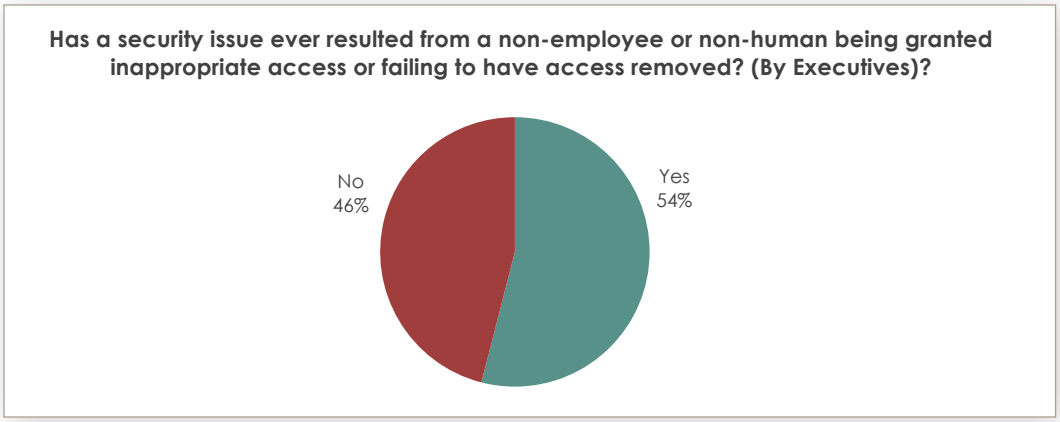
Many devices have access to company systems and data, but not just the expected traditional computers and mobile devices. For many businesses there is a host of Internet of Things (IoT) devices that can have access to manufacturing equipment, inventory scanners, RFID chips, Point of Purchase devices, card readers, and more. All of those devices need to have access to the network, key applications, and related data.

Perhaps less obvious to those outside of IT is the basic fact that today's modern software architecture utilizes supporting applications and services that can be internal to the company or external through cloud services or SaaS applications. As a result, applications are integrated with other software and access must be granted to share data between them. This survey finds that 88% of companies provide access to non-humans that interface with their applications and systems to provide and receive data.



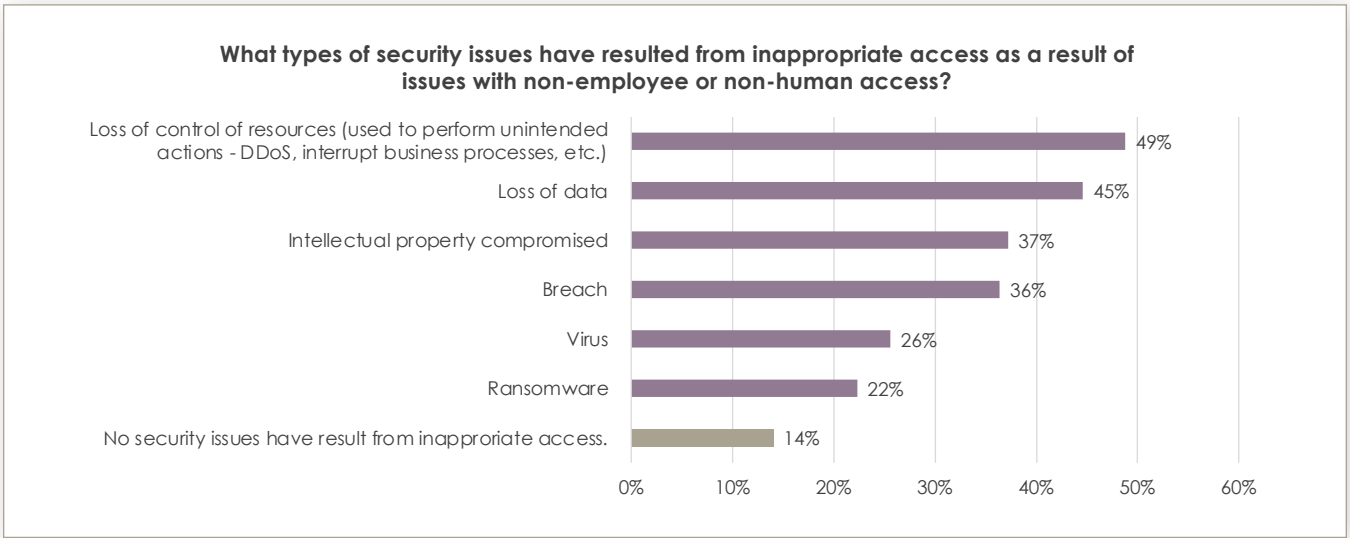
Most Companies Experience Security Issues from Inappropriate Access

The bottom line is that providing access to non-employees and non-humans is now a common business practice and a necessity but granting and managing access incorrectly poses a tremendous business risk. More than half (54%) of executives shared that inappropriate access privileges have resulted in a security event for their company.



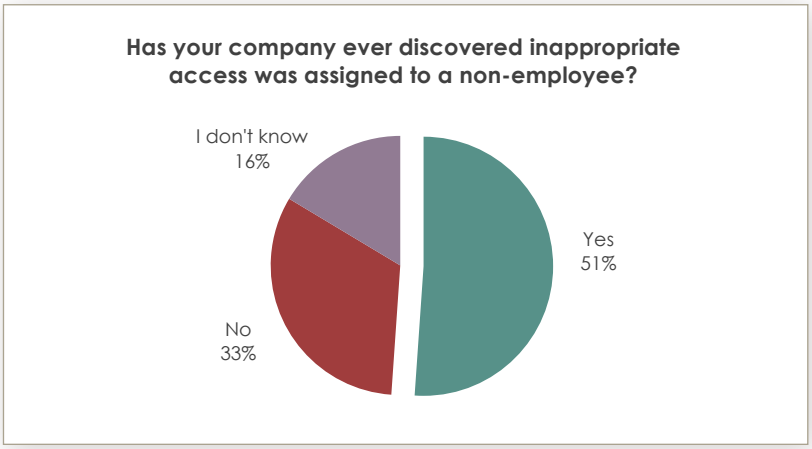
Inappropriate Access Results in Breaches, Loss of Control of Resources, Data, and Intellectual Property

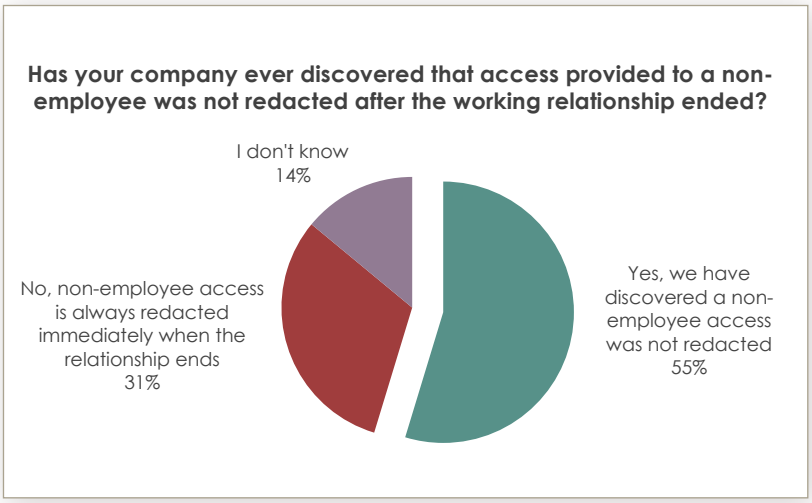
Security issues arising from inappropriate access are severe, with nearly half (49%) reporting the loss of control of resources (infrastructure, applications, etc.), not only interrupting the business but resulting in the potential for those resources to be used to commit additional security attacks both internally and externally. Loss of data (45%) carries the potential for operational issues, compliance problems, impacting your customers, and tarnishing a company's brand. Intellectual property compromises (37%) and ransomware (22%) are direct attacks on the business itself., and a full security breach occurred for 36% of participants, resulting from mismanagement of identities and access.



Granting Inappropriate Access to Non-Employees Is Common

More than half (51%) of companies admit that inappropriate access has been granted to non-employees. Also concerning is the 16% who don't know, which indicates a lack of visibility and governance, with the reality that business-impacting activities could be occurring now without anyone's knowledge. Again, more than half (55%) of those surveyed revealed that access was not revoked after the working relationship ended for a non-employee. This open door of access is a risk to disgruntled individuals and those who can exploit those access privileges.





SailPoint Non-Employee Risk Management provides organizations with a powerful identity security solution that extends advanced governance controls to large and complex populations of non-employee users, including contractors, partners, seasonal workers, franchisees, affiliates, vendors, virtual workers, etc.

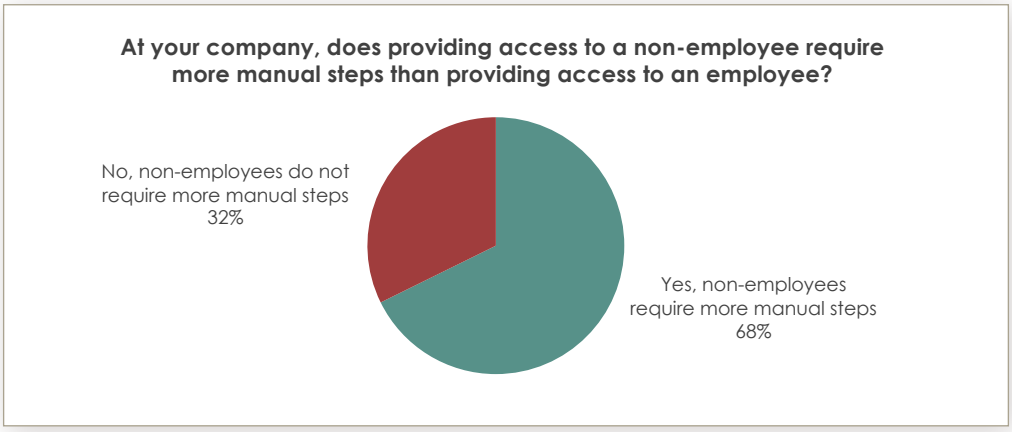
By leveraging automation and AI functionality, organizations can increase operational efficiency while managing the complex relationships that they have with non-employees in an easy-to-use solution that simultaneously helps facilitate commercial initiatives, supports regulatory compliance, and reduces third-party risk.

- View, identify, and track a non-employee's relationship with your organization to determine why access is required.
- Utilize flexible workflows for all lifecycle management events, and securely automate identity processes.
- Eliminate time-consuming processes with an easy-to-use tool using a drag-and-drop configuration.
- Execute risk-based identity and access lifecycle strategies to mitigate risk of a third-party breach with individual identity risk scoring.

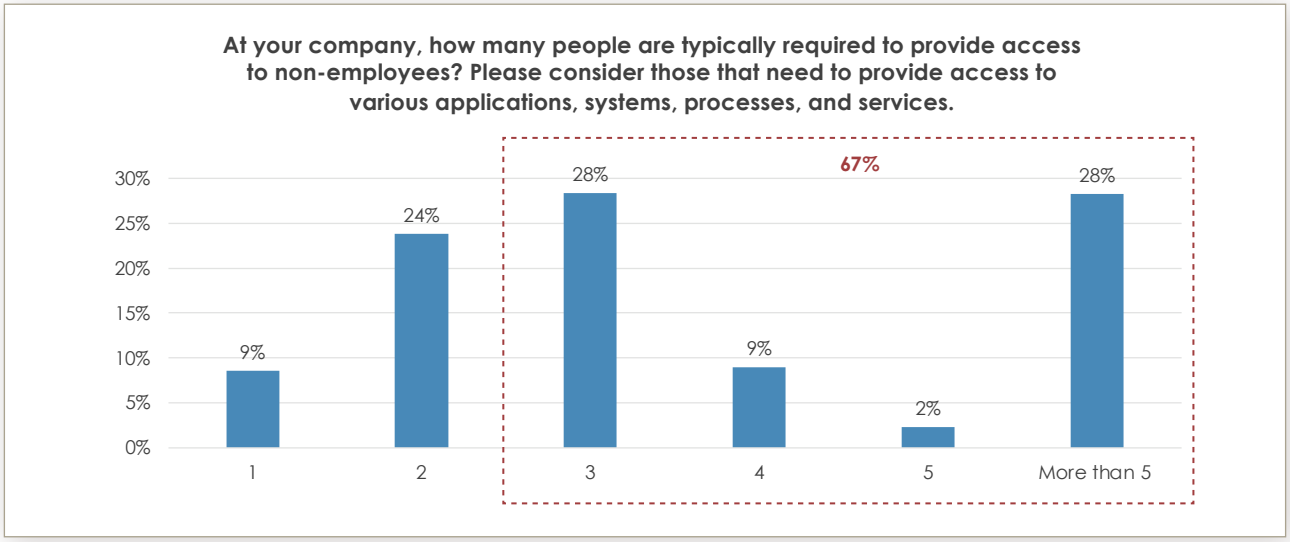
With SailPoint Non-Employee Risk Management, organizations can easily manage the simplest to the most complex scenarios when it comes to non-employee identities the same way it manages employee identities.

Providing Access to Non-Employees is Difficult

With the frequency and ramifications of inappropriate access being covered, the research then investigated the potential causes for the mismanagement of access for non-employees. Nearly 7 in 10 participants shared that providing access to non-employees requires more manual steps than providing access to an employee, creating increased time requirements and risk of error.

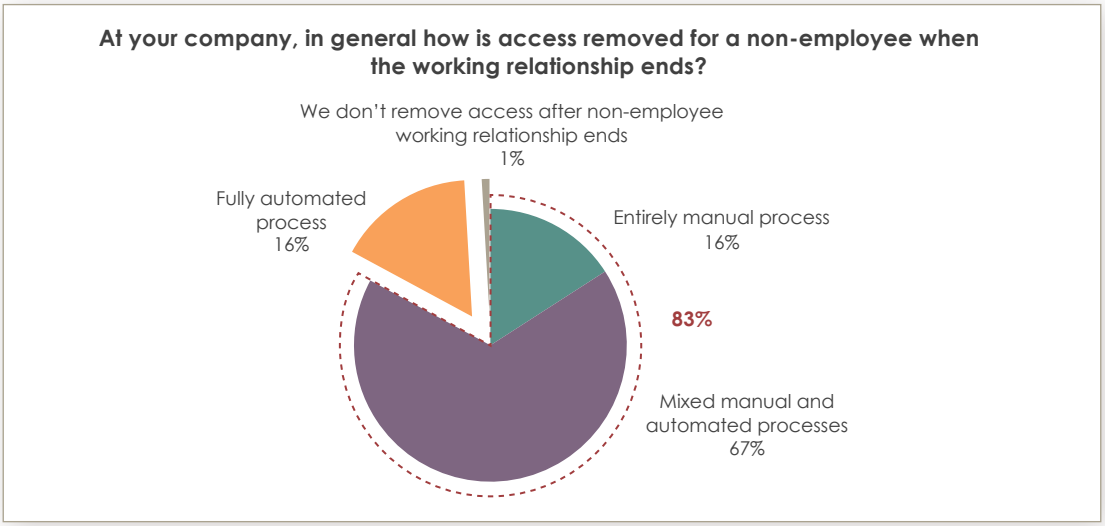


Additionally, 67% of companies require 3 or more individuals to be involved in providing access for non-employees, and 30% require 5 or more people. These many handoffs create opportunity for process errors that are compounded by the fact that most of it is manually performed.



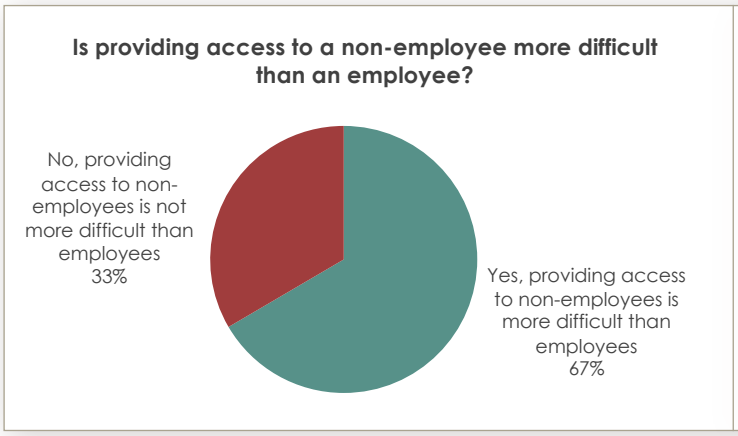
Companies Rely on Manual Processes to Remove Identities and Access

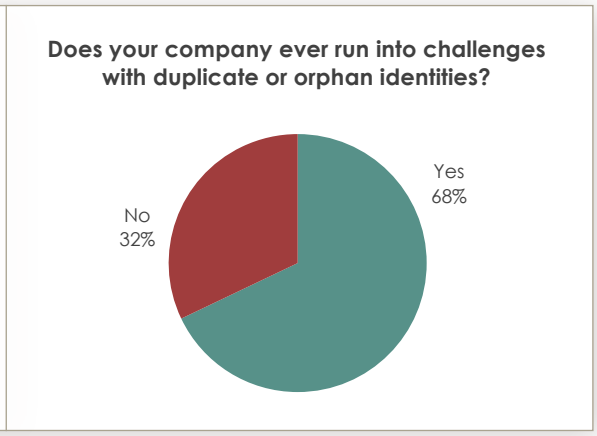
The preceding section proved it is difficult and resource intensive to grant access to non-employees. The research also finds it is just as difficult to remove access once the relationship ends, 83% reported it also requires manual steps and processes to remove access. This high effort may be a reason so many companies reported earlier that access often remains after a non-employee has finished and left.



Manual Access Processes Breed Duplicate and Orphaned Identities

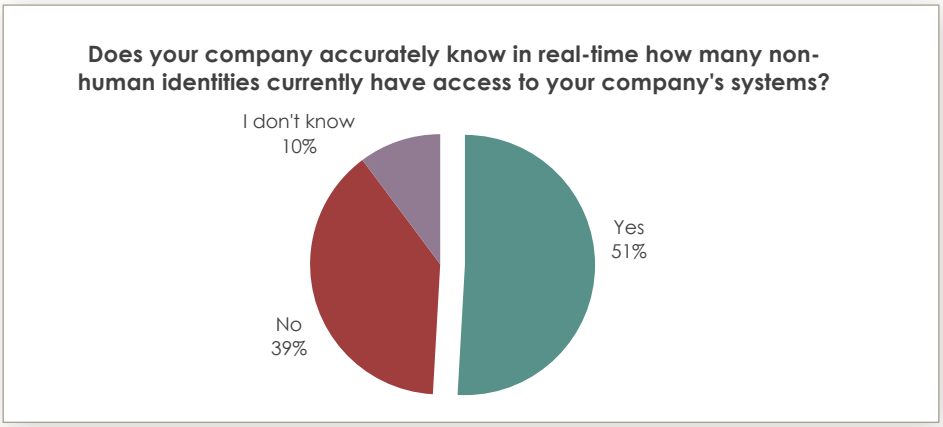
The impact of manual-laden processes involving numerous employees results in 67% directly stating that managing access for a non-employee is more challenging than for an employee. These challenges and manual efforts have unfortunately led to the practice that only 33% fully delete an identity and related access once the relationship ends, and most simply disable the identity and/or the corresponding access. However, that low effort approach has led to 68% of companies reporting issues with duplicate and orphaned identities. Those duplicate and orphaned identities create an identity management nightmare and additional opportunities for exploitation.



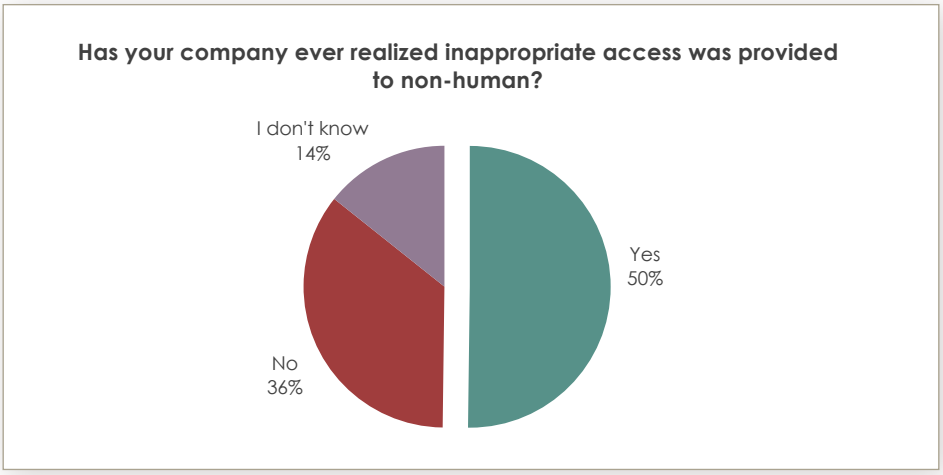


Many Don't Know Which Applications, Services, or Devices are Accessing Their Systems

At the start of the report, we discussed the necessity and prevalence of non-human access. However, barely half (51%) of companies know in real-time how many non-humans have access to their systems. If you don't know what is accessing your systems, you likely don't know what they are accessing either. With the rise in software supply chain security issues, the risk further grows that a device or applications are accessing inappropriate data.

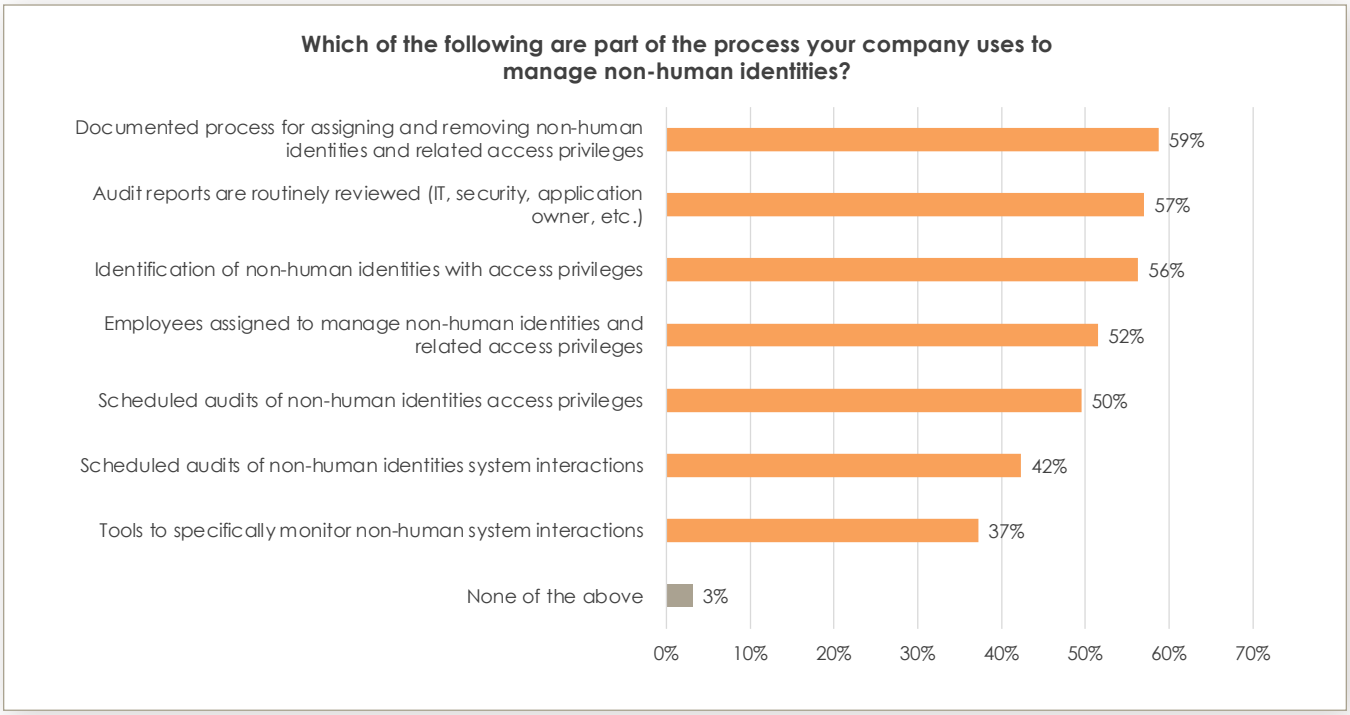


That concern is validated in that 50% of companies have realized that inappropriate access has been granted to a non-human. Another 14% don't know if they have allowed unauthorized access, and not knowing can be riskier or can perpetuate undiscovered risk. Similar to providing access to non-employees, the research finds that non-human access also requires lengthy processes with numerous individuals and the low-effort approach of just disabling the identity or access but not fully deleting it when access to a device or service is no longer needed.



Companies Need Proven Approaches to Managing Non-Human Identities

With the growing use of business devices, integrated services, and applications, we asked identity professionals which approaches they are using to manage non-human identities. Typically, research reveals one or two dominant approaches which establish themselves as the best practices. However, in the chart below the top 5 answers are only separated by 9%, indicating a lack of best practices and indicative of a developing market. The top 5 are all valuable with documenting processes (59%), audit reports (57%), identification of non-human access (56%), assigning non-human identities as a specific job responsibility (52%), and regular audits of existing access privileges (50%) currently in use. But it is clear from the chart and preceding finding that companies are struggling with an effective way to manage non-human identities and access.



Conclusion

Creating identities and granting access to non-employees and non-humans is a business necessity. However, the research shows it is being managed poorly. The risk of inappropriately-privileged identities causing serious business issues is not a threat that may happen in the future, but is an unpleasant reality for the majority of companies. With new growing threats like software supply chain security or identity focused exploits the risks will grow.

That challenge of managing identities and access today for nearly all companies both requires a multitude of manual steps and a lot of human resource interaction. Both create an opportunity for error, delays, and extra work. The manual work that occurs for every non-human or non-employee has led to weak practices about reviewing, deleting identities, and access privileges, which is directly fueling risk and having business impact.

Ironically, the most obvious answer, which was NOT in the top seven approaches currently used to managing non-human access is utilizing automation. An automated approach to auditing current non-employee identities and their access is an obvious start. Then flagging identities that have not utilized access for several weeks to ensure contractors whose relationship with your organization has ended are removed.

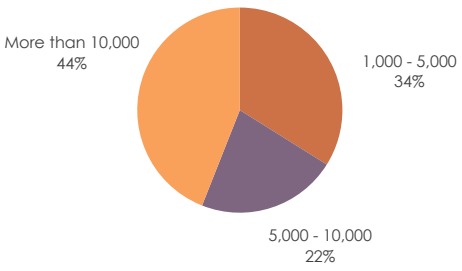
Just those few simple approaches would go a long way to improving the management of identities and access, not to mention the benefit of unloading the manual processes and related workloads from your company's most valuable assets.

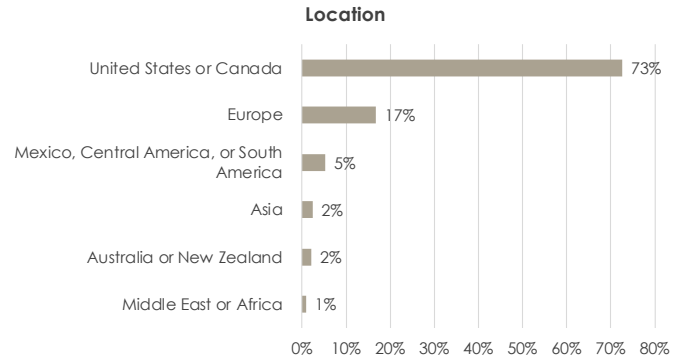
Moving forward, organizations would be wise to consider platforms that are specifically built for non-employee and non-human identity management. A purpose-built system should eliminate over-provisioning and untimely de-provisioning and reduce risk, giving organizations more transparency and control over their non-employee resources. As a result, organizations could lower labor-related costs for access and issue remediate as well as making well-informed, risk-based decisions about access, ultimately reducing the risk of security breaches.

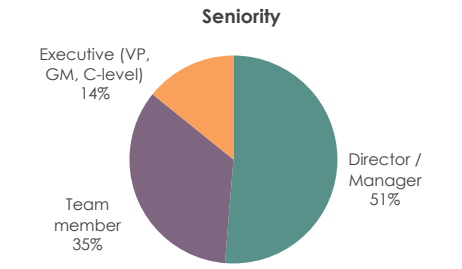
Survey Methodology

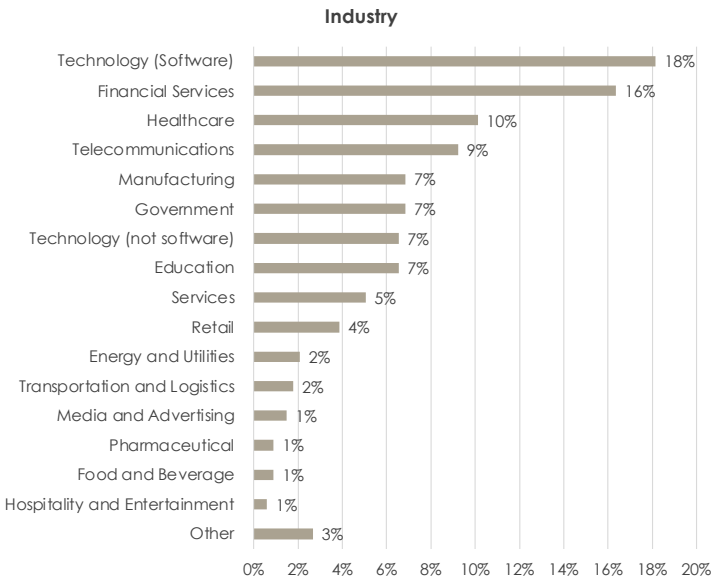
This data was compiled from Security and IT professionals at enterprise companies representing all seniority levels. These professionals were invited to participate in a survey on their company's identity and access practices.

A total of **339 qualified participants** completed the survey. All participants had direct identity and access responsibilities or managed teams that did so. Participants were from 5 continents, providing a global viewpoint. The survey was administered electronically, and participants were offered token compensation for their participation.









About Dimensional Research

Dimensional Research provides practical marketing research to help technology companies make their customers more successful. Our researchers are experts in the people, processes, and technology of corporate IT and understand how IT organizations operate. We partner with our clients to deliver actionable information that reduces risks, increases customer satisfaction, and grows the business.

For more information, visit www.dimensionalresearch.com.

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.

For more information, visit www.sailpoint.com.