Identity and Access Management: The Stakeholder Perspective

A survey of HR, Sales, and Help Desk Professionals

Limited for distribution by Identity Defined Security Alliance members only.

Portions of this document may be reproduced with the following attribution:
Identity Defined Security Alliance, www.idsalliance.org. *Identity and Access Management: The Stakeholder Perspective*

dimensional research

Sponsored by IDENTITY DEFINED SECURITY ALLIANCE

Introduction

With the number of identities in the enterprise exploding, the processes and technologies for managing them have become increasingly important. While granting system access to new workers in a timely manner enables business operations to run smoothly, failing to revoke system access in a timely manner opens up organizations to risk. Delays in removing access for departing workers or current workers displaying suspicious behavior can mean compliance violations or the worst case scenarios, stolen credentials or theft of confidential information.

Understanding and solving the challenges around access management is essential for businesses. Yet, while security and compliance research typically focuses on the identity and access management (IAM) and security teams, little attention is paid to the business stakeholders -- HR, Sales, and Help Desk professionals -- who are impacted by IAM processes and technologies and who interact directly with workers to set up, remove, and resolve access problems.

In this new research, the Identity Defined Security Alliance (IDSA) and Dimensional Research sought to capture hard data on the experiences of these stakeholders and the impact of current practices on security risks and business operations. As insider and external threat actors alike continue to try to abuse user access to steal data, how the following questions are answered directly influences not just worker productivity, but also the risk profile of the entire organization. How long does it take to grant or revoke required access? Do you immediately remove access upon an employee's termination? Have former employees ever taken company information without authorization when they left?

For this study, we focused on three specific types of stakeholders:

- HR professionals who oversee the workers that join the company, move to different areas of the company, or eventually depart the organization
- Sales Managers to represent the business teams who are concerned about productivity and sensitivity of the data being accessed
- Help Desk teams who handle access requests, access removals, and resolve access problems

The following report, sponsored by the IDSA, is based on an online survey of 313 qualified professionals. All participants worked at a company with at least 1,000 employees where a typical employee required access to multiple systems to do their work. Participants in this study all had direct responsibility for adding or removing access to corporate systems in an HR, Sales Manager, or Help Desk role.

© 2021 Dimensional Research.
All Rights Reserved.

Identity and Access Management: The Stakeholder Perspective

A survey of HR, Sales, and Help Desk Professionals

Dimensional Research | February 2021

Key Findings

- **System access creates challenges**
  - 72% report it takes at least a week for a typical worker to get access to required systems
  - 50% report it usually takes three days or longer to revoke access for a worker that leaves
  - One in five Sales Managers report situations where it took a month or more to revoke access
  - 83% say Covid-19 has made system access more difficult
- **Stakeholders are invested in security, but poor behaviors still exist**
  - 81% believe they share responsibility for access issues
  - 56% of Sales Managers report they had staff who stole information when they left
  - Only 38% would immediately terminate access based on suspicious behavior
  - Seven in 10 confess to having personally engaged in poor system identity behavior
  - 68% prioritize getting their job done over security
- **System access processes and technology have room for improvement**
  - 78% report there is more than one department involved in defining system access
  - Two in five characterize ownership of system access as "messy and all over the place"
  - Only 23% report system access enablement is automated
  - Only 35% report revoking system access is automated
  - 83% say access request processes could be improved

DEFINITIONS GIVEN SURVEY PARTICIPANTS

"Corporate systems" refers to any systems, data, or applications a worker might need to access. This includes HR systems (payroll, benefits, company portal, etc.), email, collaboration (Microsoft Teams, Slack, Zoom, WebEx, etc.), cloud-based productivity (Google Apps, Office 365, etc.), file sharing and storage (network drives, DropBox, Google Drive, etc.), role specific (Salesforce/CRM, ERP, etc.), and more.

"Worker" includes any employee, contractor, vendor, or other individual who requires access to your company's corporate systems in order to do their work.

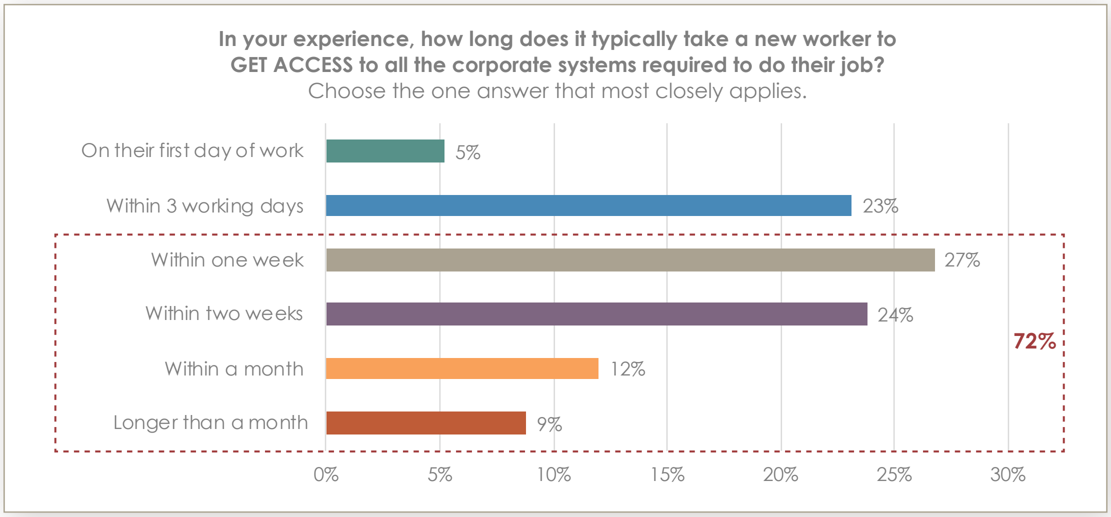
© 2021 Dimensional Research.
All Rights Reserved.

Detailed Findings: Access challenges continue to exist

New hire system access is frequently slow

With the high reliance of today's businesses on technology, workers cannot be productive without access to corporate systems. From email and messaging for communication, to enterprise applications that knowledge workers use throughout their day, to time tracking apps that frontline workers use to log their hours, if a worker is not able to use systems, they are typically not able to deliver their full value.

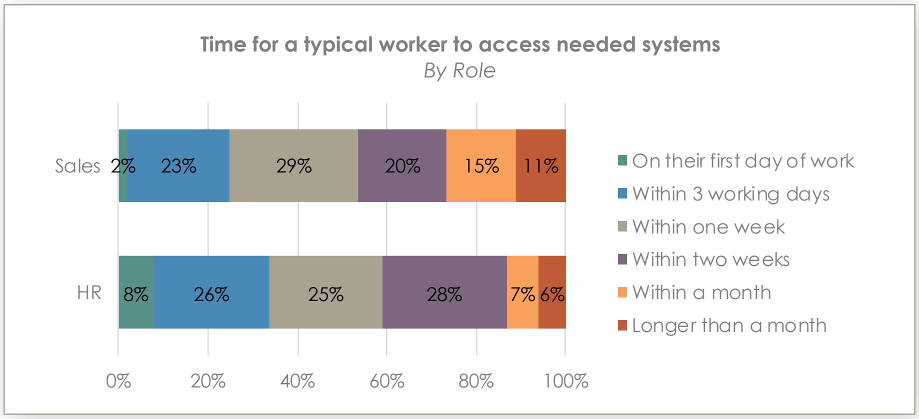
It is possible that there may be little business impact for taking a little bit of extra time to enable new workers. New hires could be in training or shadowing someone who does have access to needed systems. However, this research clearly demonstrates that few companies succeed in getting their new workers up and running efficiently. Only 28% report that a typical worker can access all corporate systems required to do their job within three working days. This number includes only a tiny percentage (5%) that actually have met the goal of having a typical worker up and running on day one. For the large majority of companies (72%), it takes a week or even longer. Worrisomely, it is not at all exceptional (21%) for a typical new worker to have to wait for a month or even longer to gain access and become productive.



© 2021 Dimensional Research.
All Rights Reserved.

It is important to note that this research considered only the systems that workers required to do the work they were hired to do. There is no expectation that all systems that may be available to a worker should be available immediately after being hired.

All organizations within a company will likely not have an equivalent need for system access. For example, sales teams that use a wide variety of systems to manage customer interactions, conduct meetings, book and track orders, and collaborate with internal teams may have more complex system needs than a facilities team that works primarily with a scheduling system. The data in this study confirms that the delay in accessing needed systems is particularly noticeable among Sales Managers, with three-quarters (75%) reporting that it takes a week or more to grant access compared to just two-thirds (66%) of HR stakeholders who are responsible for a wide range of worker roles.



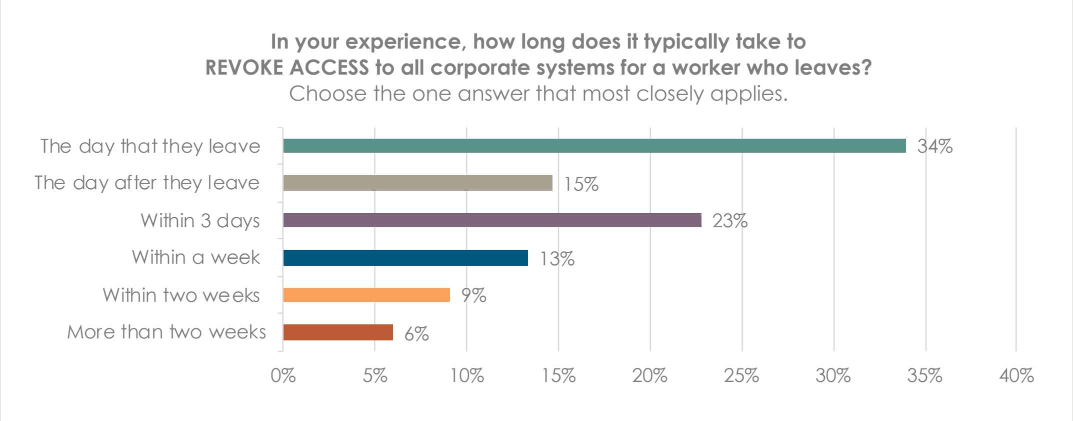
© 2021 Dimensional Research.
All Rights Reserved.

Revoking system access can take days or longer

When workers are first brought into a team, productivity is the primary driver for timely system access. But when they leave, the concern becomes even more pressing - protecting key systems and confidential data by quickly and completely revoking access to systems. A delay in revoking system access can lead to data theft, even in circumstances where the employee has left on their terms, as well as the risk of a regulatory compliance violation. And of course, if the worker is fired, the potential for intentional damage increases dramatically. Quickly ending access to corporate systems is vital. The standard among security teams is that all system access for exiting workers should be revoked immediately.

This research shows that few companies are meeting this security standard. Only a third (34%) report that a typical worker has their access revoked the day they leave. Half (50%) of companies take 3 days or longer to revoke access.

It is particularly concerning to see that well over a quarter (28%) take a week or even longer to revoke access, enabling far too much time for a disgruntled employee to do damage.



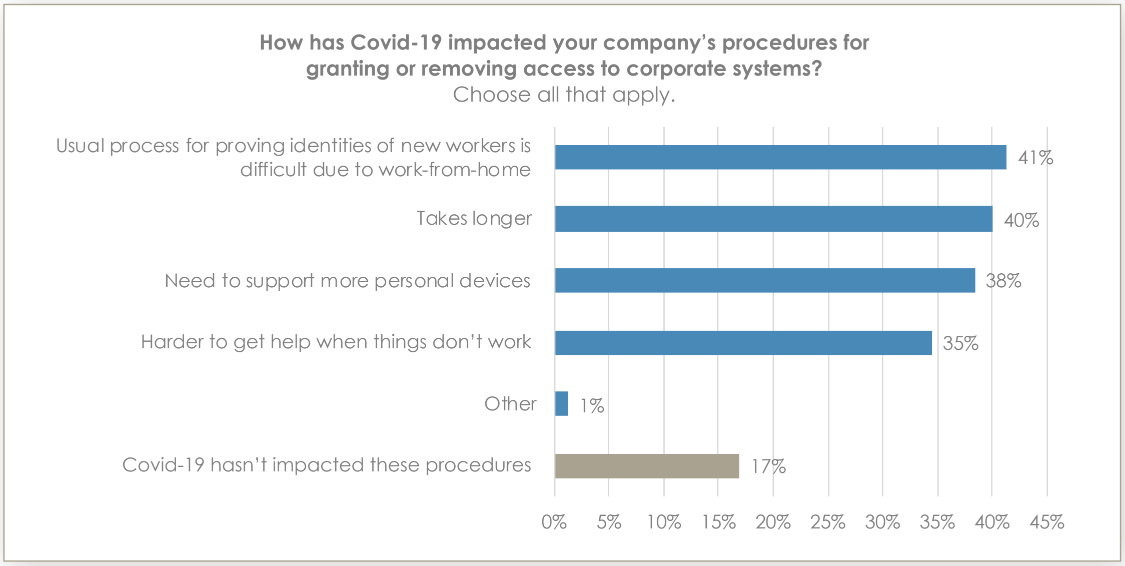
This study also asked about the longest time it has taken to revoke access to an employee. Among Sales Managers, an alarming one in five (19%) reported scenarios where it had taken over a month to revoke access for employees who had left the company.

© 2021 Dimensional Research.
All Rights Reserved.

Covid-19 has added to the challenges of system access

It cannot be overstated how Covid-19 has impacted every area of life in the past year. System access is no exception. Practically overnight, IT organizations were forced to provide remote access to workers who previously worked in an office. In the name of productivity, workers accessed corporate applications and data from personal devices and, in some cases, unprotected Wi-Fi networks, creating access challenges and security risks. Formerly simple steps in the onboarding process, such as bringing in a government-issued ID as proof of identity, suddenly became much harder and introduced risk.

The majority (83%) of system access stakeholders report that remote work, social distancing measures, and other Covid-19 related factors have impacted how their company manages access to corporate systems. Proving identities for new workers has been complicated due to work-from-home (41%), gaining and revoking access is taking longer than before (40%), there is a need to support more personal devices (38%), and most importantly, it is harder to get help when things don't work (35%). Several participants took the time to write in "other" factors, including an HR professional that reported the new connectivity protocols that don't always work, a Help Desk worker that reported needing to support a wider range of device types, including more Apple-based equipment, and a Sales Manager that could no longer just walk over and talk to the Help Desk to resolve a problem.



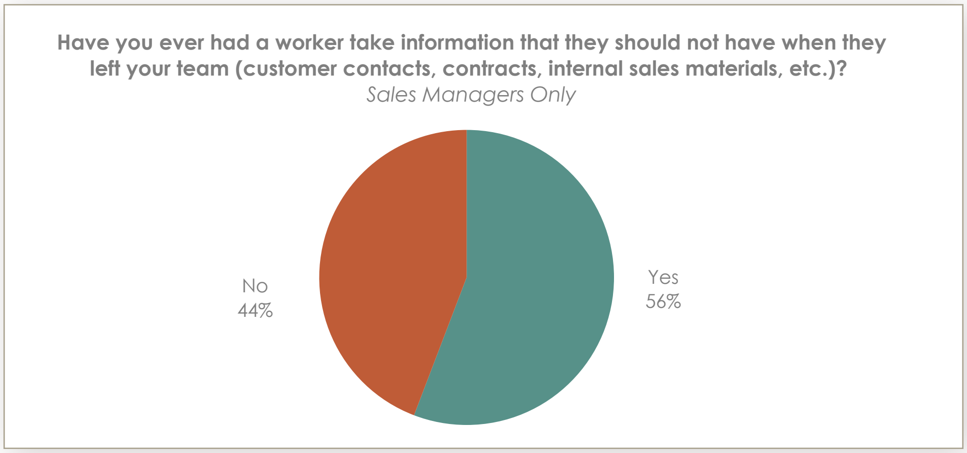
© 2021 Dimensional Research.
All Rights Reserved.

Detailed Findings: Stakeholders are invested in security, but bad behaviors still exist

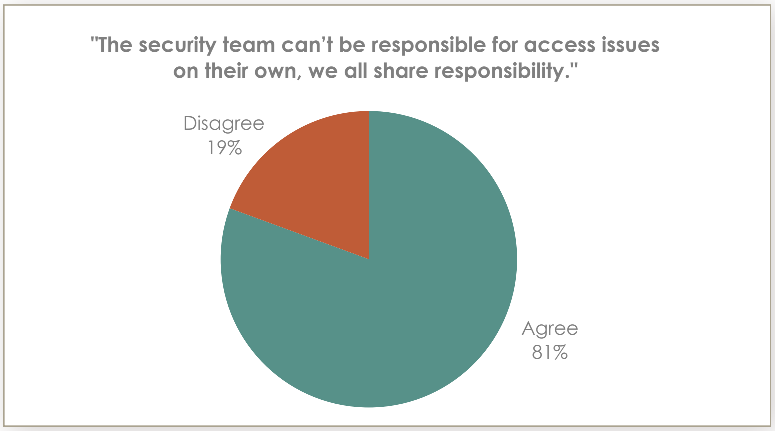
Security is everyone's job

Any worker access to corporate systems includes risks. Workers must have this access to do their jobs, but it often means that they have access to confidential or sensitive information, the ability to impact processes or data quality, and the potential to accidentally infect systems by being an entry to a hack. For workers with privileged access, the risk is even higher.

A clear example of this risk was highlighted by this study. We asked Sales Managers if they ever had a worker take information when they left, with a question that focused on information that should not have been taken, such as contract details, customer contacts, or internal sales materials. Well over half (56%) said that this situation had happened to them, and this number may be even higher since sales staff might have taken information without their manager becoming aware of the theft.



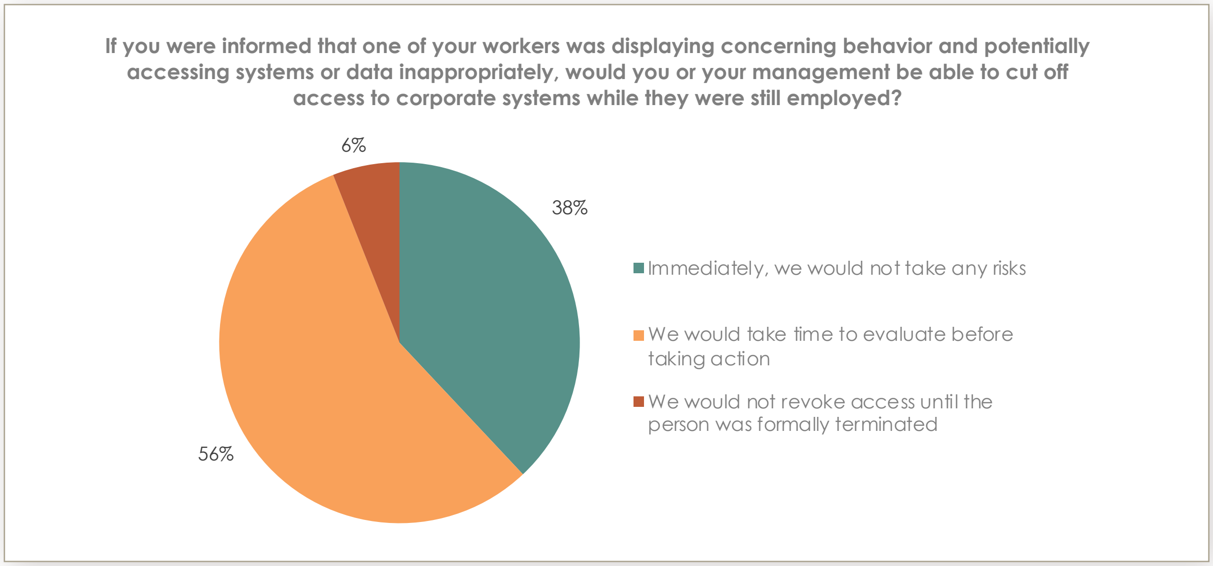
Access stakeholders are in agreement that these types of issues are not a problem just for the security team to solve; everybody has a role. More than four in five (81%) agree that responsibility is shared. This belief is held consistently across all access stakeholders — HR (75%), Sales (84%), and Help Desk (82%).



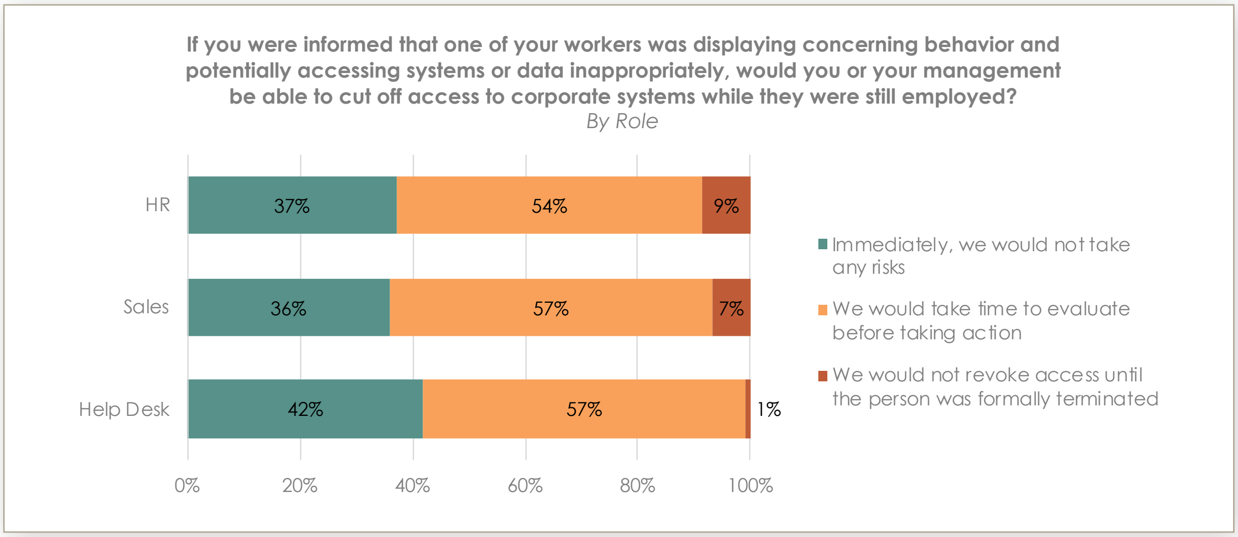
© 2021 Dimensional Research.
All Rights Reserved.

Business stakeholders often hesitate to remove access without clear proof

It is fascinating to note that despite this agreement that they have responsibility for security, most access stakeholders in this study (62%) reported that they would be hesitant to take action and cut off a worker's system access in the face of concerning behavior. Only two in five (38%) reported that they would not take any risks and would immediately cut off access for a worker who was accessing systems or data inappropriately.


If you were informed that one of your workers was displaying concerning behavior and potentially accessing systems or data inappropriately, would you or your management be able to cut off access to corporate systems while they were still employed?

Help Desk stakeholders were the most likely to report they would take immediate action on system access (42%). Some HR (9%) and Sales Managers (7%) were so uncomfortable with the idea of revoking access that they said they would wait until a worker was terminated to revoke access, probably far too late to prevent harm.


If you were informed that one of your workers was displaying concerning behavior and potentially accessing systems or data inappropriately, would you or your management be able to cut off access to corporate systems while they were still employed?
By Role

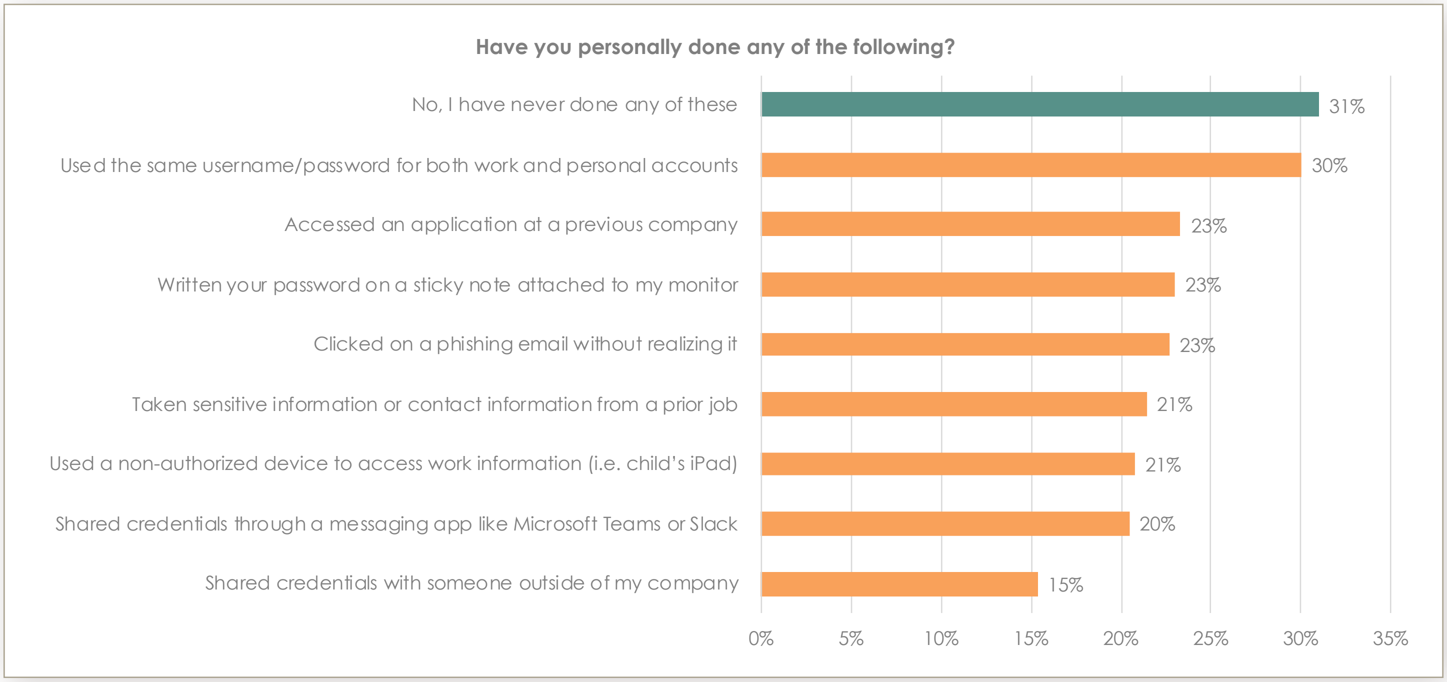
Even access stakeholders have bad behavior

The stakeholders in our study all had direct responsibility for worker access as a key part of their duties, and as we saw above, felt they had some ownership for security. It might be assumed that they would be particularly aware of good security hygiene related to their own access to corporate systems. Unfortunately, this was not the case.

To ensure participants felt comfortable sharing this information, we did remind them that their answers to the survey were completely anonymous before asking this question, and we did get honest feedback. Almost seven in 10 (69%) HR, Sales, and Help Desk stakeholders confessed to having personally engaged in questionable security behavior. The most frequently reported poor behavior was using the same username and password for both work and personal accounts (30%). Concerning behaviors reported also included putting passwords on a sticky note on their monitor (23%), clicking on a phishing email (23%), using an unauthorized device for work (21%), sharing credentials through a messaging app (20%), and sharing credentials with non-workers (15%).

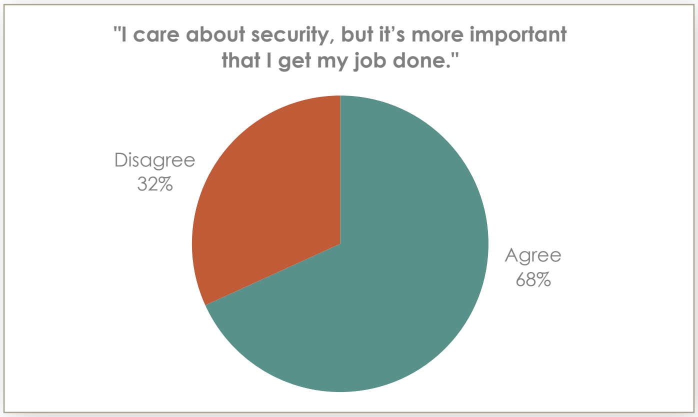
Interestingly, 23% reported accessing an application at a previous company, and 21% admitted they had taken sensitive information from a previous job, a reminder that there are consequences when system access is not revoked in a timely manner.

Worryingly, Help Desk workers, who are often responsible for implementing security policies as part of their work, were just as likely to confess to these poor identity behaviors as their HR and Sales counterparts in this study!



© 2021 Dimensional Research.
All Rights Reserved.

Part of the explanation for this behavior may come from the continued attitude that security takes second place to job performance. Well over two-thirds (68%) agreed that even though they care about security, it is more important to get their job done. This attitude was particularly prevalent among Sales Managers (72%).



Detailed Findings: Identity teams have room for improvement

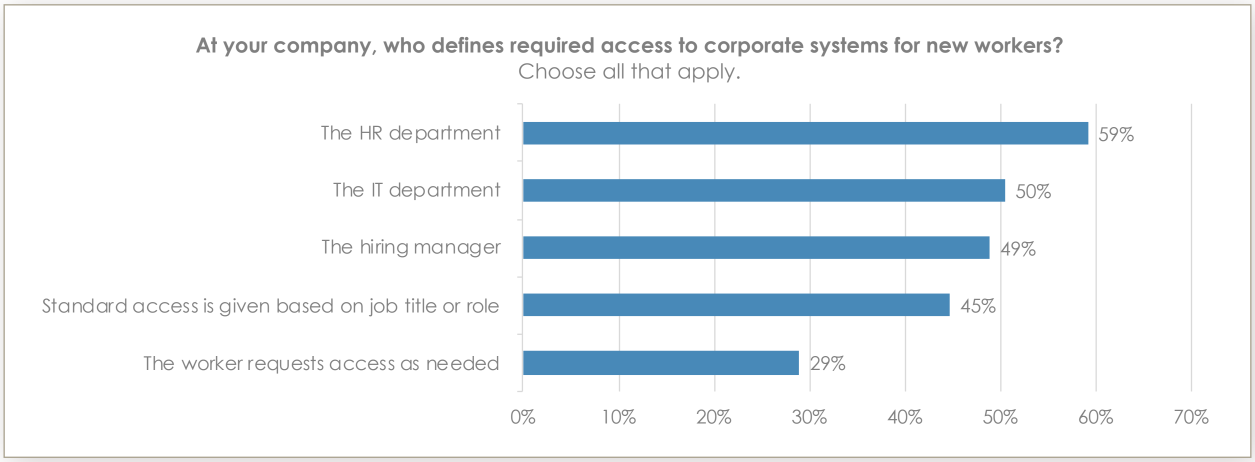
Ownership is complicated, and processes are not automated

When looking for a reason for the delays in granting and revoking worker access, two main challenges appear. The first is a lack of clear ownership, and the second is a lack of automation.

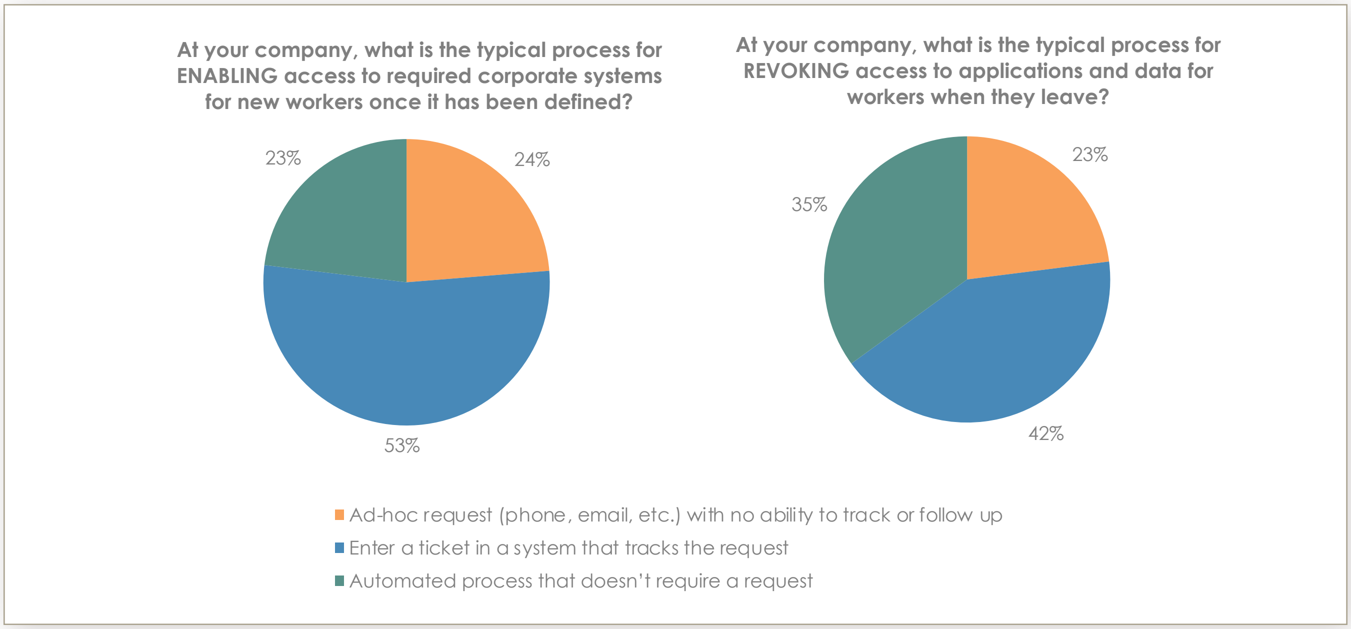
It is not unusual that access to corporate systems involves multiple perspectives. When asked who defines required access to corporate systems, answers vary from HR (59%), IT (50%), the hiring manager like the Sales Managers in this study (49%), or even the worker who is required to request the access they need (29%). Just under half (45%) report that their company grants standard access based on job title or role.

© 2021 Dimensional Research.
All Rights Reserved.

It is not concerning in and of itself that there are multiple teams involved in defining access to corporate systems. But when there are "too many cooks in the kitchen," it can cause conflicting decision-making and delays, or potentially result in the over-provisioning of access which bloats the cyber threat surface. In this study, more than three quarters (78%) reported more than one answer when asked who defines access.

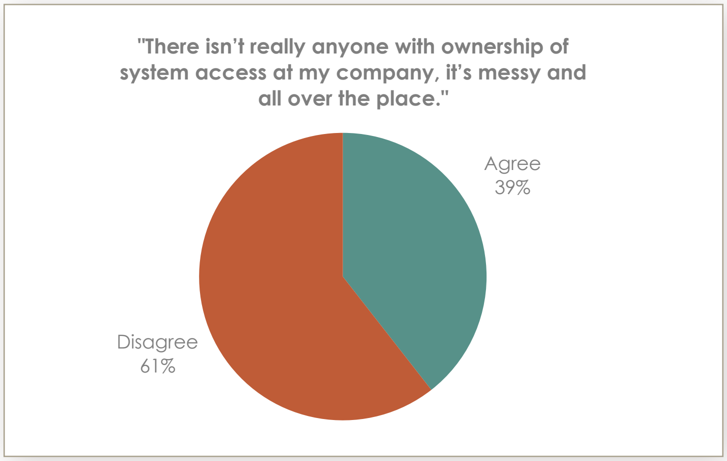

At your company, who defines required access to corporate systems for new workers?
Choose all that apply.

The second data point that jumps out when looking at why there are delays in granting and revoking access is the lack of automation. Less than a quarter (23%) report that they automate enabling access to required corporate systems, while only a third (35%) report automation of revoking access when workers leave.


At your company, what is the typical process for ENABLING access to required corporate systems for new workers once it has been defined?

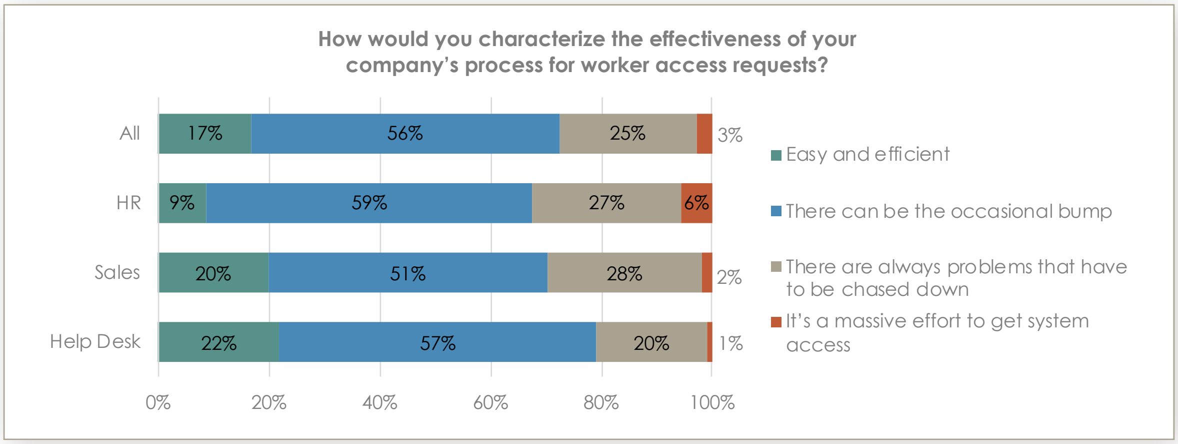
At your company, what is the typical process for REVOKING access to applications and data for workers when they leave?

Given these ownership and automation issues, it is not surprising that two in five (39%) agreed that system access at their company is "messy."



Access stakeholders want improvements to system access

The HR, Sales, and Help Desk stakeholders in our study are consistent (83%) in their belief that system access can be better. Only 17% report that their current process for requests is "easy and efficient," which should be the standard.



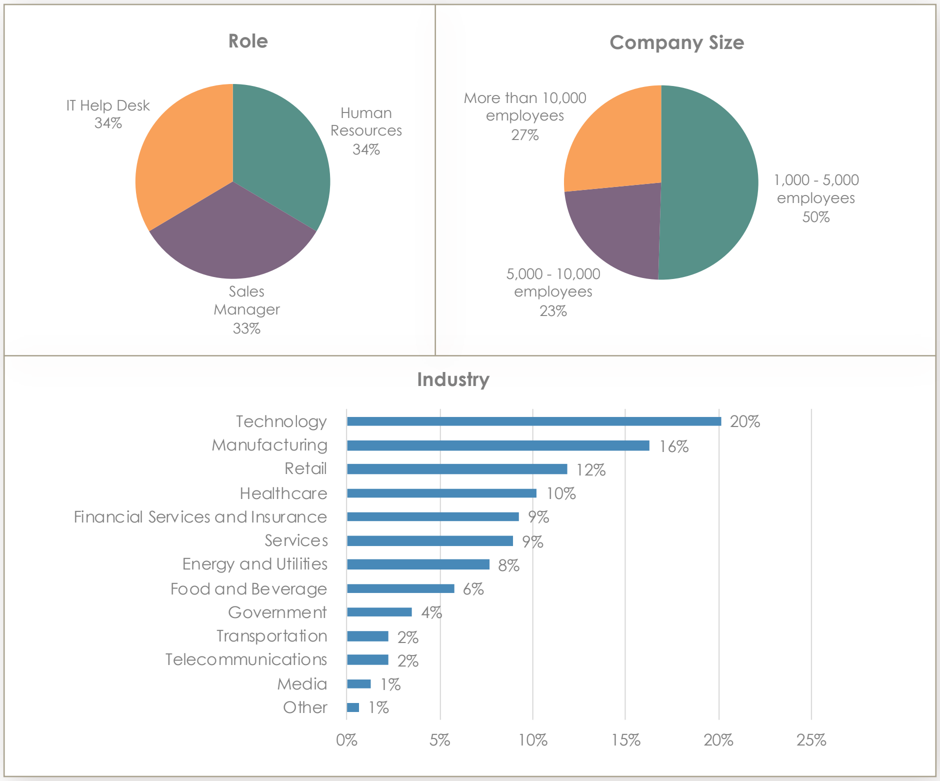
© 2021 Dimensional Research.
All Rights Reserved.

Survey Methodology and Participant Demographics

An online survey was fielded to independent sources of HR, Sales, and Help Desk professionals in the United States. A total of 313 qualified professionals completed the survey. All participants worked at a company with at least 1,000 employees where a typical employee required access to multiple systems to do their work. Survey participants in this study all had direct responsibility for adding or removing access to corporate systems in one of the following roles:

- 105 HR professionals responsible for new hire onboarding
- 103 Sales Managers who had hired five or more workers in the past year
- 105 Help Desk staff who respond to access tickets or requests

Certain questions were worded slightly differently based on roles while remaining similar enough to compare answers. The survey was in the field collecting data from December 17, 2020 to January 4, 2021. Participants included a mix of roles and industries.



© 2021 Dimensional Research.
All Rights Reserved.

About Dimensional Research

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

About the ISDA

The IDSA is a group of identity and security vendors, solution providers, and practitioners that acts as an independent source of thought leadership, expertise, and practical guidance on identity-centric approaches to security for technology professionals. The IDSA is a nonprofit that facilitates community collaboration to help organizations reduce risk by providing education, best practices, and resources. For more information visit www.idsalliance.org.