THE STATE OF IDENTITY:
HOW SECURITY TEAMS ARE ADDRESSING RISK

A SURVEY OF SECURITY DECISION MAKERS

December 2019

dimensional research

Sponsored by IDENTITY DEFINED SECURITY ALLIANCE

THE STATE OF IDENTITY: HOW SECURITY TEAMS ARE ADDRESSING RISK

Dimensional Research | December 2019

Introduction

Investigate any data breach, big or small, and one common theme will frequently rear its head—compromised user credentials. In the last decade, companies have invested billions of dollars in IT security solutions and identity access management (IAM) technology to safeguard their most valuable systems and data. But even with this significant investment, stolen identities remain at the heart of many breaches.

From inadvertent misuse by insiders to an external attack targeting a business partner's servers or users, there is a growing crisis around identity in the enterprise.

Why are so many companies missing the mark in effectively securing workforce identities across their organizations? Are they aware of identity-related threats? Does the team responsible for responding to identity-related breaches possess the right level of ownership, budget, and skills to prevent them? Or, are there other factors counteracting successful risk mitigation of potential identity-related attacks?

The following report, sponsored by the Identity Defined Security Alliance (IDSA), is based on an online survey of 511 IT security professionals at large companies who have leadership or technology decision-making responsibility for the security of their IT systems and data. The goal was to understand the current reality of how identity risks are addressed by security teams.

> **Definition:** For this survey, "identities" refers to any unique digital identifier, including for human users, devices, and machines (i.e., non-human network entities including processes, services, containers and hosts).

Key Findings

- **Modern technologies are driving the explosive growth of identities**
  - 52% say that identities have grown more than five-fold in the past 10 years
  - The increase in identities is driven primarily by technology changes, such as mobile devices (76%), enterprise connected devices (60%), and cloud applications (59%)
  - Other identity growth factors include more employees (57%) and an increase in employees using technology (66%),
- **Identities are increasingly important to corporate security**
  - 100% report a lack of strong IAM practices introduces security risk
  - 92% say security leadership cares more about identity management now than in the past
  - Security teams are worried about a range of potential identity-related security incidents, including phishing (83%), social engineering (70%), compromised privileged identities (64%), and more

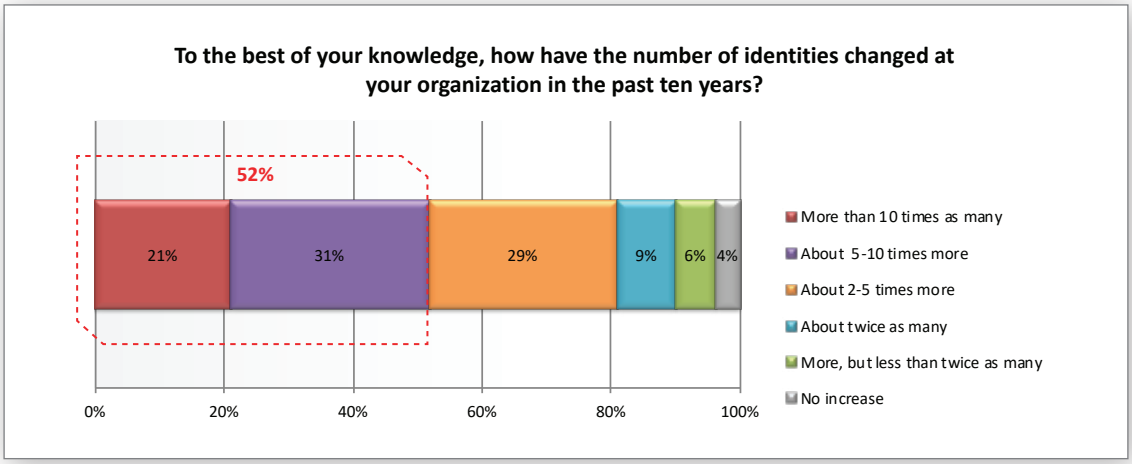
- **Identity security efforts lack alignment**
  - While security is involved in IAM activities (99%), only 24% say their security team has "excellent" awareness of IAM
  - A wide range of organizational issues prevent security from engaging with workforce IAM, including lack of alignment of goals (33%), reporting structure (30%), history of security not being involved (30%), and resistance from existing teams (24%)
  - Budget ownership issues (40%) are cited as the top reason for not spending more on workforce IAM
- **Incomplete security ownership for identities has consequences**
  - Only half (53%) report that security has any level of ownership for workforce IAM
  - When security teams have ownership of IAM they have a better understanding of identities, are more likely to view IAM leadership as a career opportunity, and face fewer barriers to IAM involvement

Detailed Findings: Modern technologies are driving the explosive growth in identities

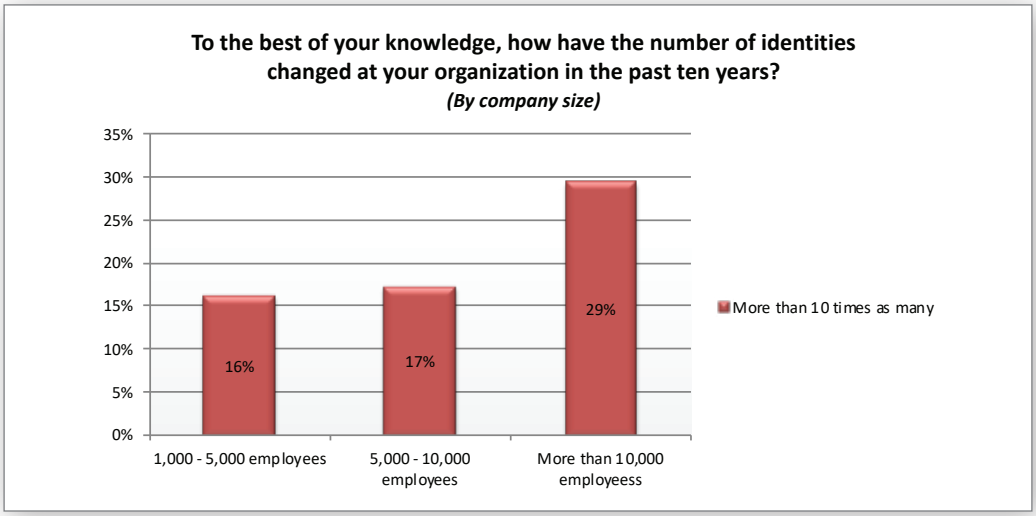
Workforce identities have grown more than five-fold in the past decade

Digital transformation is driving change throughout the enterprise, from the pace of software development to the adoption of Internet of Things (IoT) technologies. However, those changes often directly impact identity management by creating new interdependencies between platforms and increasing the number of human users, applications, and devices accessing enterprise systems.

When we asked IT security professionals about how their number of identities have changed in the past decade, more than 81% say that their number of identities has at least doubled. This includes more than half (52%) who report it has grown more than five-fold, a dramatic level of growth in only ten years!



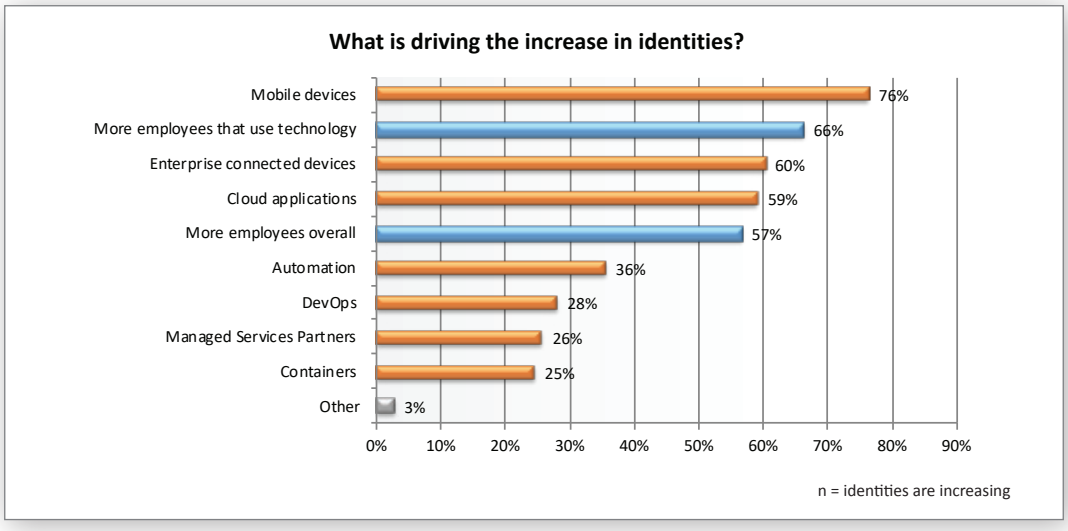
Identity growth is particularly aggressive at the largest companies. Close to a third (29%) of companies with more than 10,000 employees cite an increase of ten-fold in identities almost twice that of companies with only 1,000 to 5,000 employees (16%).



Adoption of modern technologies combined with the growth of connected employees are driving increase in identities

What is fueling this explosive growth in identities? IT security professionals shared a mix of responses, but with two overarching themes: adoption of new technologies and increased employee use. On the technology front, mobile devices (76%) was the most common response, followed by enterprise-connected devices (60%), cloud applications (59%), automation (36%), and containers (25%). In addition, 57% cited an overall increase in the number of employees and 66% stated more employees were using technology.

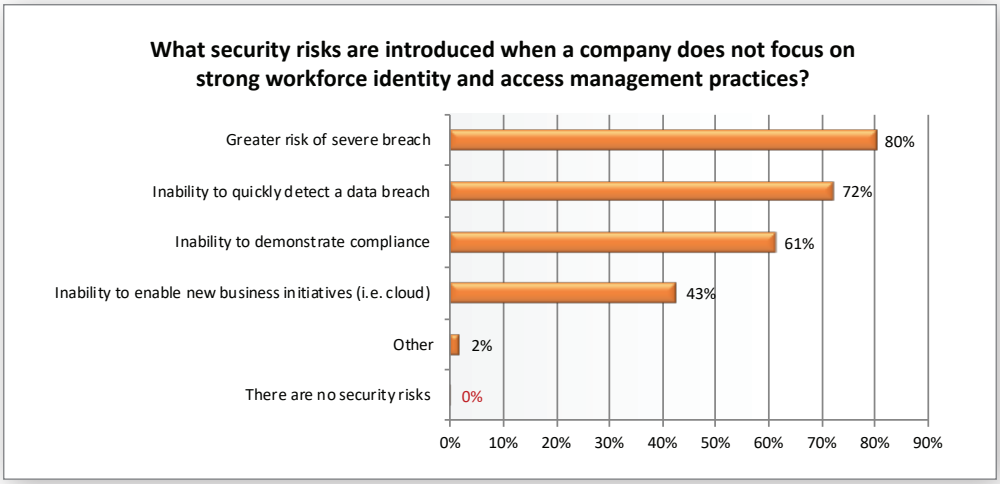
It's also interesting to note those respondents who took the time to emphasize identity growth drivers in the "other" section of this question. Those responses included mergers, acquisitions, policy changes, segregating services, and integrated applications that need logins to each other.



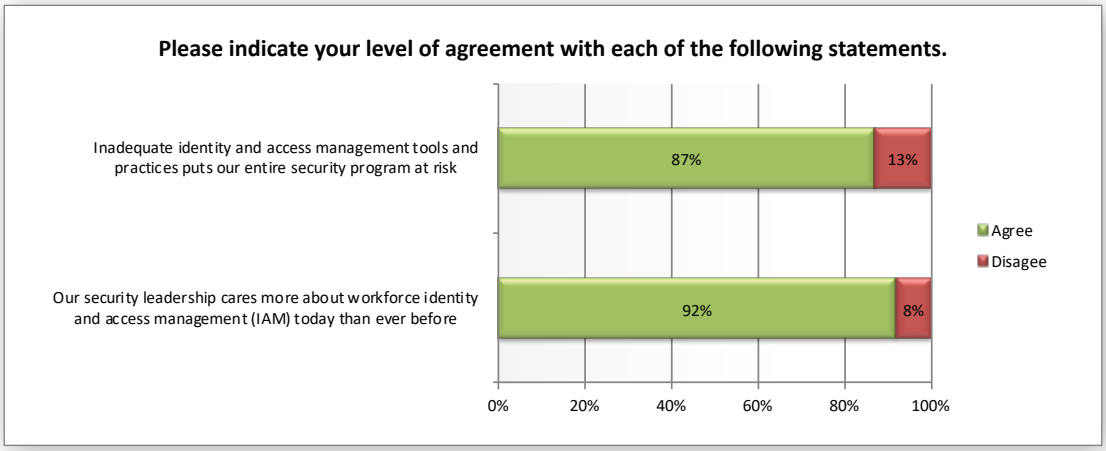
Detailed findings: Identities are increasingly important to corporate security

There is a growing awareness of the impact IAM has on security posture

With the number of users and devices exploding, identity management has grown significantly more complex. To gain a better understanding of the importance of IAM in corporate security, we asked a series of questions related to current IAM practices. Unsurprisingly, every security professional (100%) reported that lack of strong IAM practices introduces some form of risk. An overwhelming 80% of IT security professionals affirm that there is a greater risk of a severe breach to an organization when there is not a focus on strong workforce IAM practices. In addition, 72% say the absence of good IAM practices will hinder an organization's ability to quickly detect a data breach altogether. A few respondents also took the time to mention loss of business, difficulty in managing incidents, and the inability to trace violations to an individual as "other" types of possible security risks due to insufficient IAM practices.

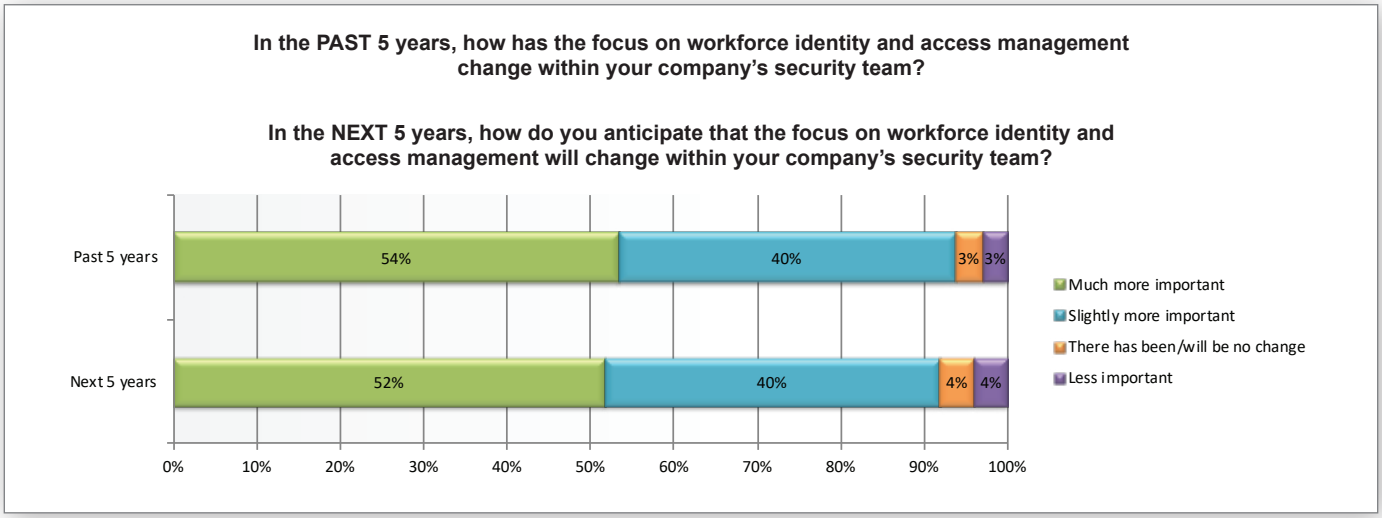


The majority of security professionals (87%) agreed that inadequate IAM tools and practices can jeopardize an overall security program.

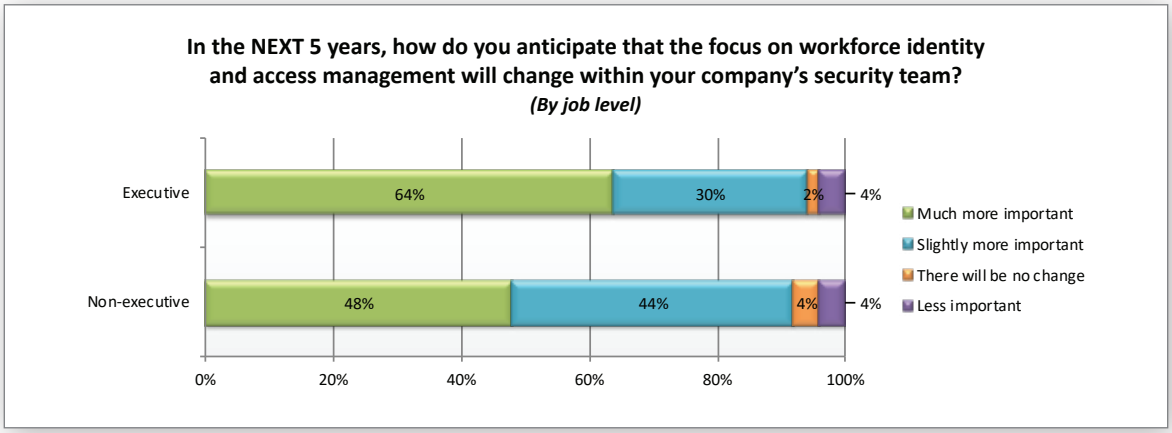


The challenges revealed by the respondents are not lost on security leaders. One of the positive takeaways of this survey is the overwhelming majority (92%) of IT security professionals say their security leadership cares more about identity management now than in the past.

When asked about how their focus on IAM is changing throughout the entire security team, we see similar levels of changing importance as reflected among security leadership. Most security professionals (94%) say IAM is more important to their team today than it was five years ago, including more than half (54%) who characterize the difference as "much more important." And this focus will not slow down. A similar majority (92%) anticipate it will continue to increase in importance to the organization over the next five years.



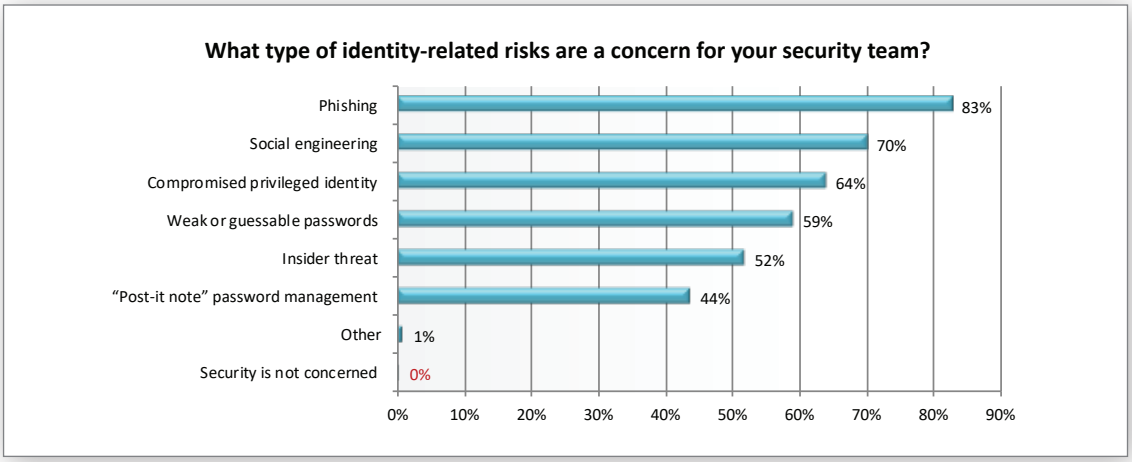
The expected growth in importance is particularly high among executives. Almost two-thirds (64%) of executives who are held accountable for their companies' reputation and profitability predict that workforce identity and access management to be "much more important" in the next five years.



Security teams worry about a wide range of potential identity-related risks

The combination of an increasing workforce of users accessing enterprise systems and the adoption of new technologies broadens the threat landscape and raises the risk of identity-related security attacks.

IT security teams are very aware of this issue, with all (100%) reporting that their teams are concerned about identity-related risks. When asked what specific types of identity issues are most worrisome for their teams, the top identity-related risk is phishing (83%) followed by social engineering (70%), compromised privileged identity (64%), and more. "Other" issues shared by respondents in this question range from shared accounts to privilege creep to terminated users.

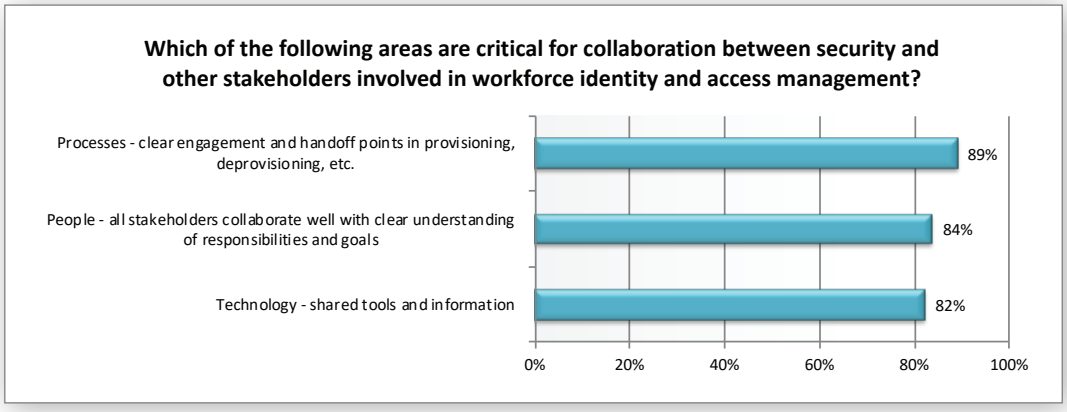


Detailed Findings: Identity security efforts lack alignment

Collaboration is critical to IAM security

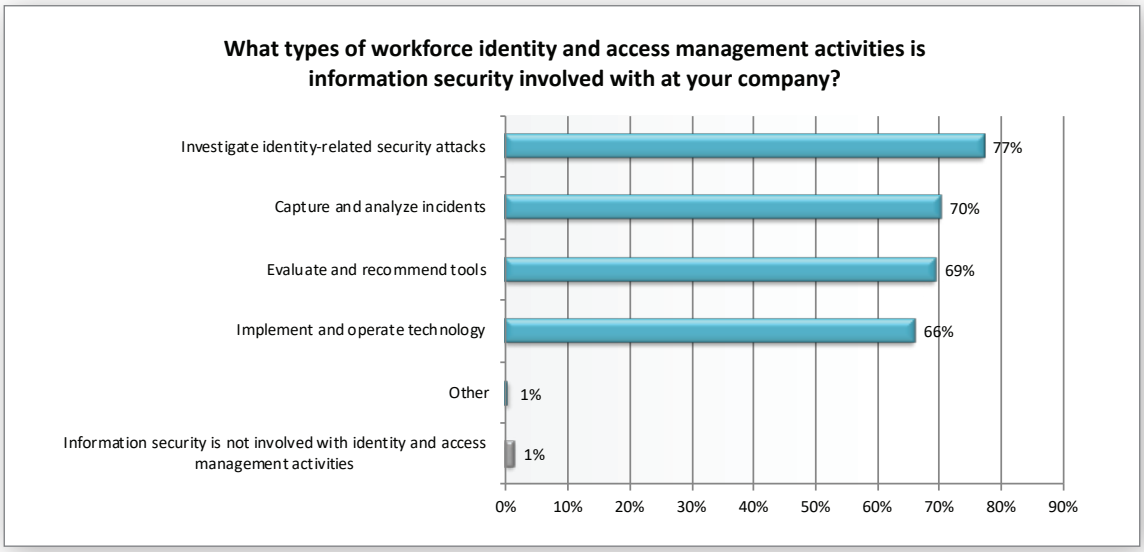
For many organizations, IAM is a shared initiative with distributed responsibilities across IT operations, IT security, HR, line managers, a dedicated IAM team, and more. To be successful, strong leadership is needed now more than ever to facilitate effective collaboration between security and other stakeholders.

According to IT security professionals, critical areas of collaboration include processes (89%) with clear engagement and handoff, its people with their responsibilities and goals (84%), as well as the technology (82%) enabling shared tools and information.

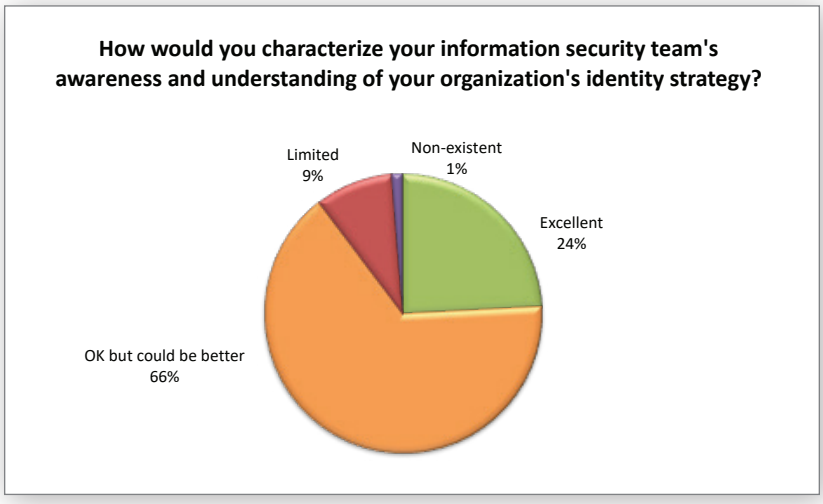


Security gets involved with IAM activities

For nearly all companies (99%), their security team is involved in a wide range of IAM activities. These include investigating identity-related security attacks (77%), capturing and analyzing incidents (70%), evaluating and recommending tools (69%), implementing and operating technology (66%), and more.



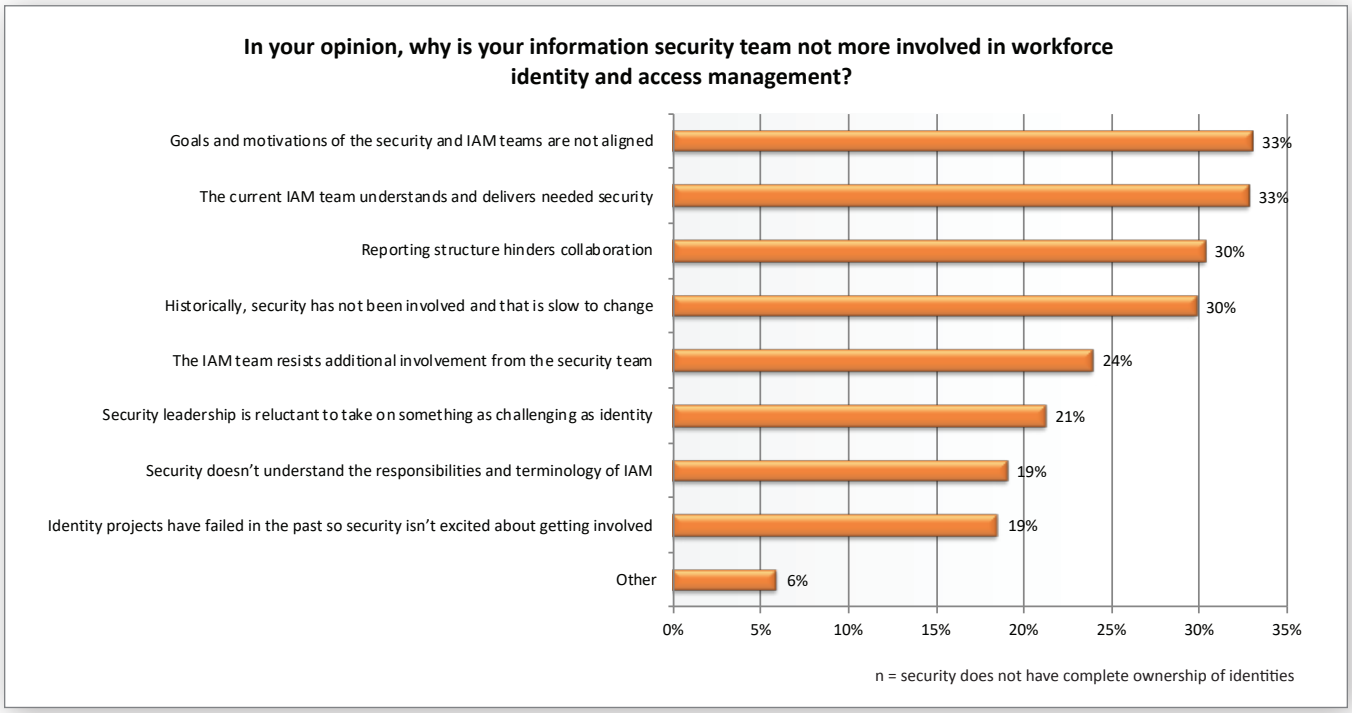
While security does participate in IAM activities, it is disconcerting that less than one in four (24%) of IT security professionals characterize their teams awareness of their company's identity strategy as "excellent."



Multiple issues prevent security from fully engaging with workforce IAM

Most surprisingly, even with the growing importance of workplace identity and access management to the enterprise, there are many issues deterring security from involvement in IAM. Of those surveyed, the top reasons mentioned are misaligned goals and motivations of IAM teams (33%), lack of understanding and delivery of needed security by the IAM team (33%), a reporting structure hindering collaboration (30%), and a history that security has not been involved (30%).

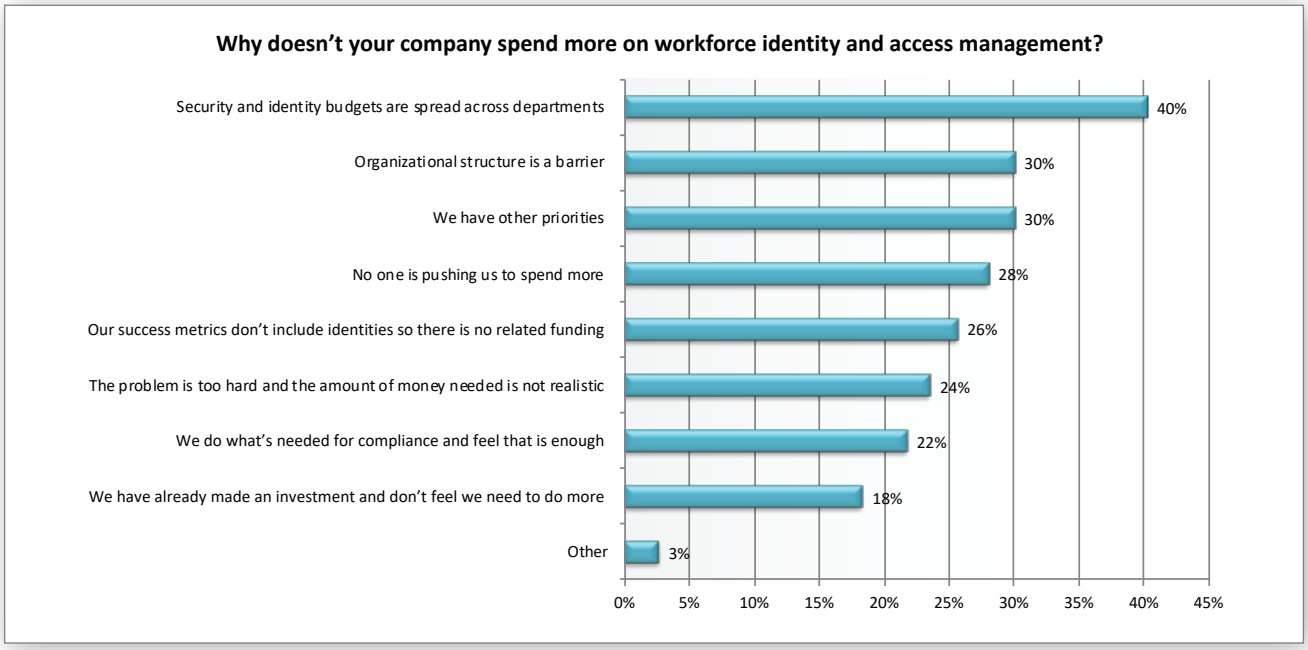
In addition, 6% of IT security professionals took the time to write in a wide range of "other" responses to this question such as a lack of support for information security needs, limited time and resources, and senior management deciding who owns IAM and not selecting security. From the severity of the responses cited, one can presume that security is not fully engaged in workforce IAM, which should be a genuine shared concern.



Siloed budgets and organizational structure prevent investment

What is one of the most detrimental effects of security teams not maintaining complete ownership of identities? No centralized ownership of budgets results in a strong limitation to investing in IAM initiatives. IT security professionals heartily agree.

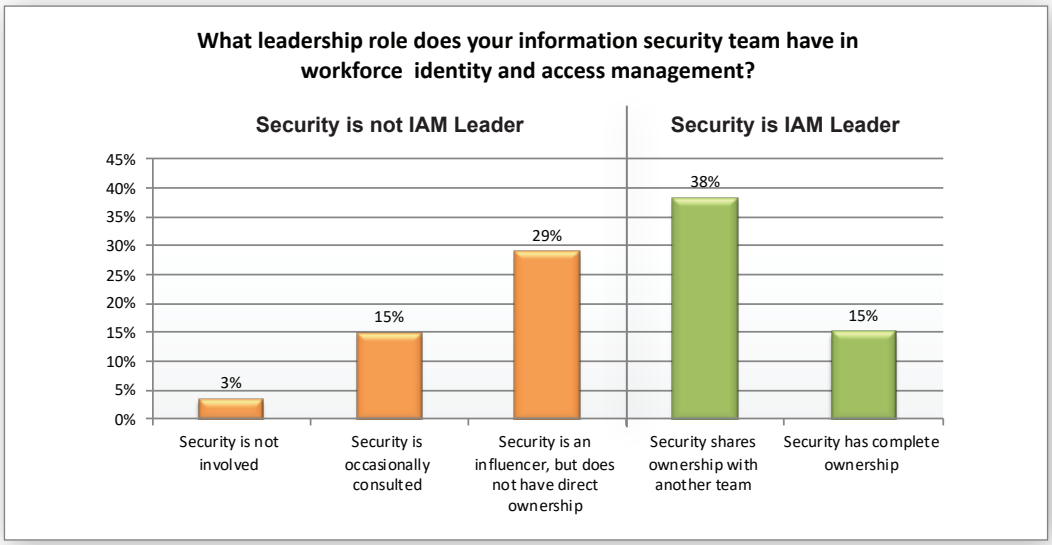
Our research found that budget ownership issues ranged from security and identity budgets spread across departments (40%) to no one pushing security to spend more (28%). Some respondents noted that their internal success metrics did not include identities so there is no related funding (26%), while others characterized the problem as being too hard and said that the amount of money needed is not realistic (24%). "Other" budget-related responses mentioned are that management doesn't see value and it is traditionally time consuming and expensive to purchase and implement workforce and identity and access management solutions.



Detailed Findings: Incomplete security ownership for identities has consequences

No standards exist for security ownership and IAM

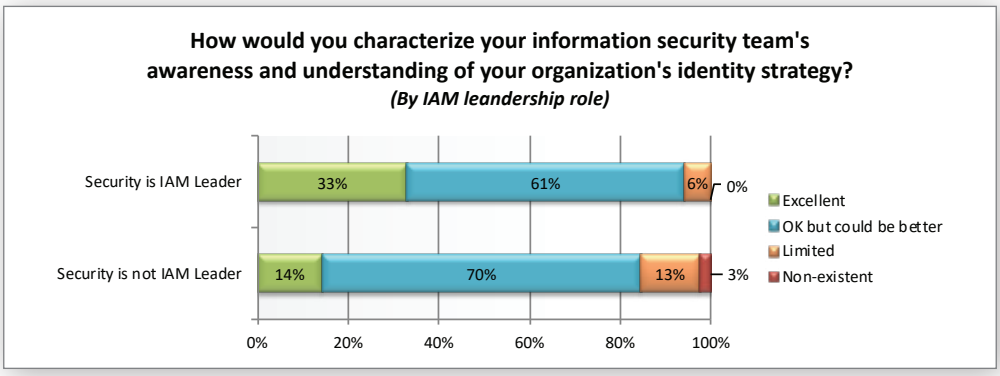
One of the most shocking findings of this study is the incongruous view about the security team's ownership role of workforce IAM. Of those surveyed, 53% say IT security is an IAM leader while 47% say IT security is not an IAM leader. This near 50/50 split indicates that companies are struggling with this decision. With only 15% reporting that security has complete ownership, this finding suggests the majority of companies are still deciding who is in control of identities and responsible for creating, establishing, and enforcing all aspects related to workforce IAM.



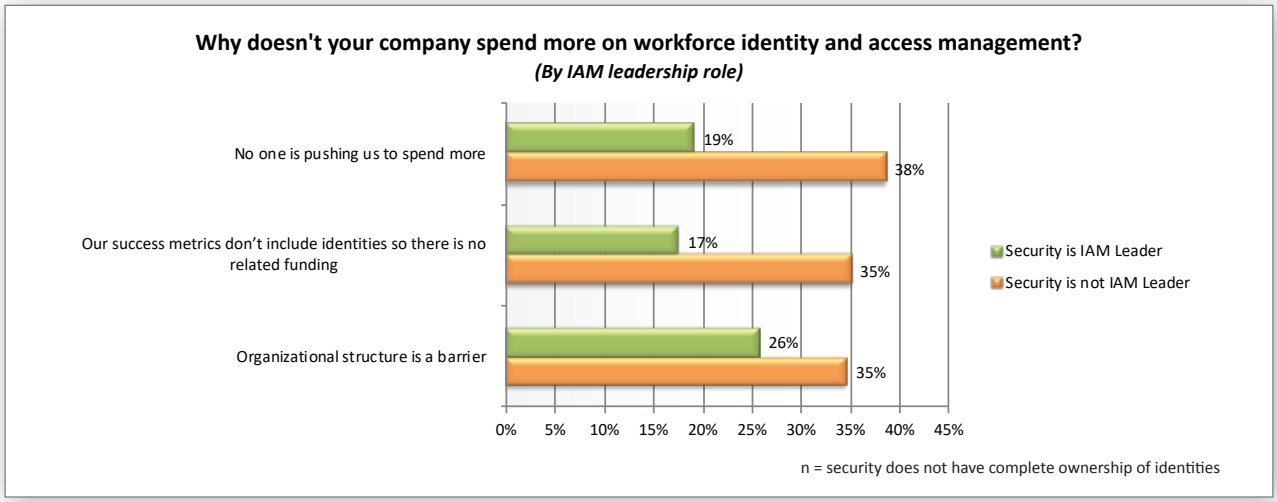
Security improves when the team takes on a leadership role

There is a notable difference in identity strategy awareness among security teams that assume leadership, with a third (33%) characterizing their security team's awareness as "excellent." At organizations where security teams do not have a leadership role with workforce IAM, that number drops significantly to just 14%.

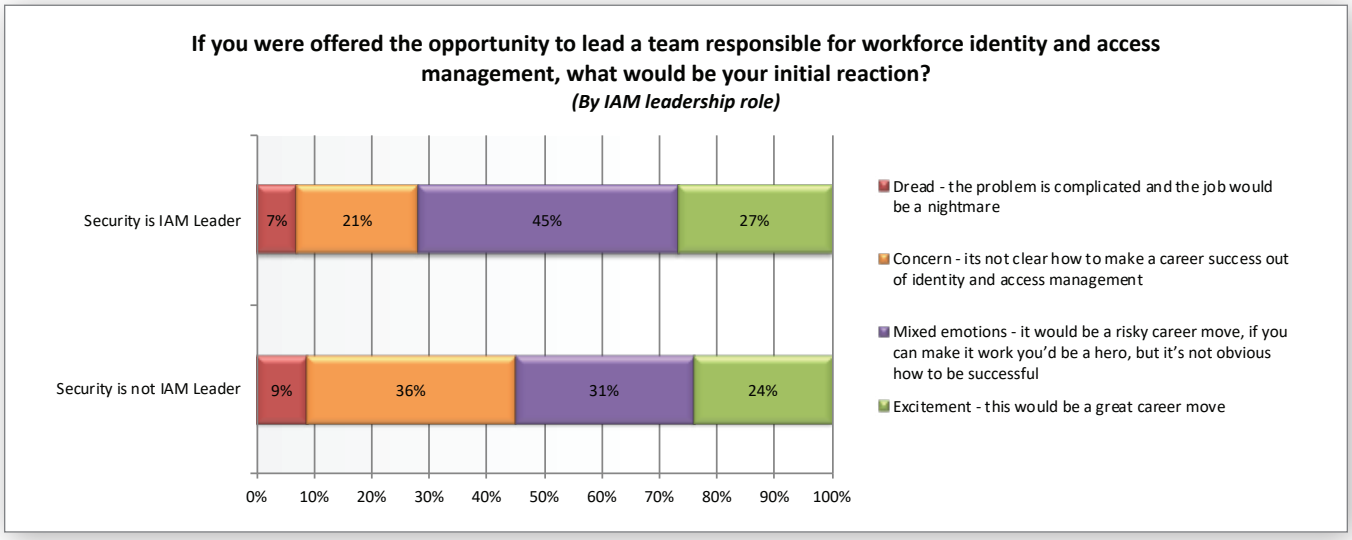
That said, when only 33% of IT security professionals give their organization's IAM leadership an "excellent" mark, there is still significant work required in order to minimize workforce identity-related risks even in companies where security has a leadership role.



Organizational changes are not a panacea and do not solve all issues. For example, challenges with budgets being spread across departments are not solved with a change in IAM leadership. But major issues including motivation, success metrics, and organizational barriers are significantly less common at companies where security has a IAM leadership role.

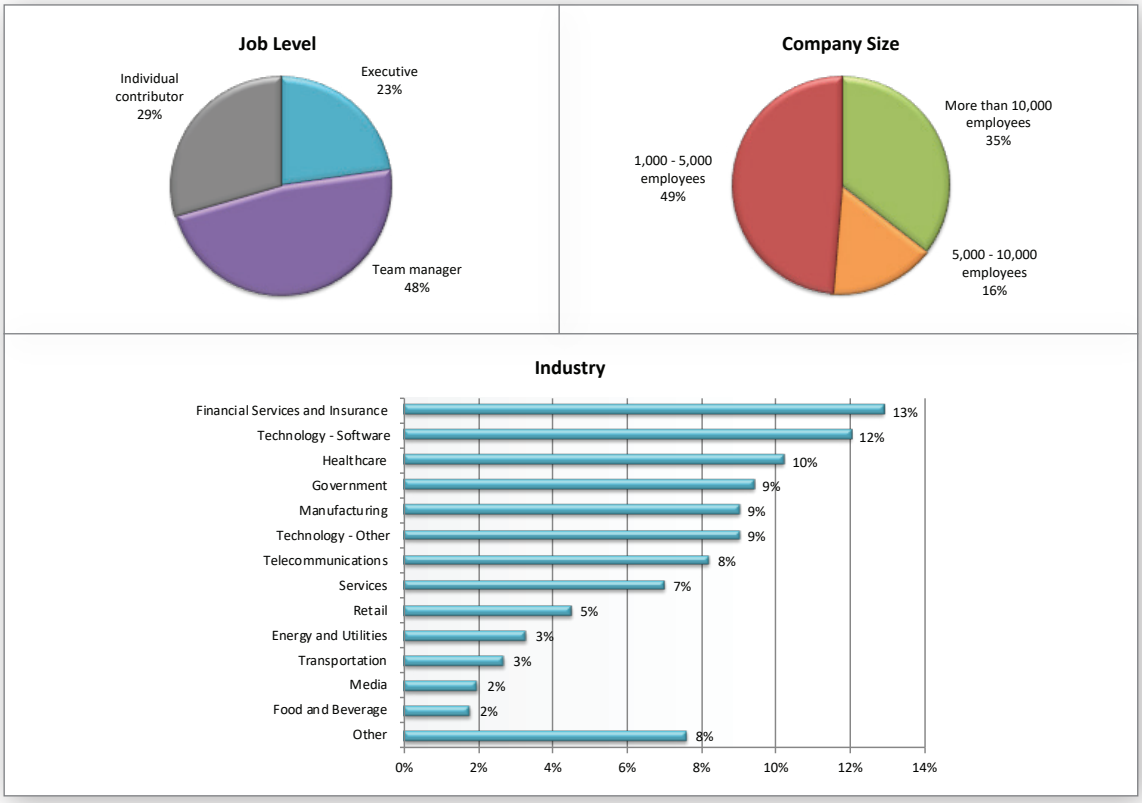


However, this isn't the end of the story. While security teams with complete ownership of workforce IAM hold a better understanding, they don't always want to lead it. In fact, only about one in four IT security professionals are excited to consider an IAM leadership role. Many respondents expressed concerns about the impact such a move would have on their career. But consider if more security professionals accept leadership roles, it may encourage amazing security employees to step up for the job. While it remains a hard problem to resolve, there will be an obvious shift from concern to possibility, which increases the likelihood of recruiting a great individual to lead IAM practices across the enterprise.



Survey Methodology and Participant Demographics

In October 2019, an online survey was sent to an independent database of IT security professionals. The focus of this survey was on workforce identity and access management as it relates to employees and partners accessing enterprise systems, not external customers. A total of 511 qualified individuals from the United States completed the survey. All worked at companies with more than 1,000 employees and had responsibility for IT security decision making. Participants included a mix of job levels in decision making, company sizes, and verticals.



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 IDSA

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.