IDENTITY SECURITY: A WORK IN PROGRESS

A Survey of IT Security and Identity Professionals

dimensional research

Sponsored by IDENTITY DEFINED SECURITY ALLIANCE

Introduction

The number of workforce identities in the enterprise is growing at lightning speed with no slowdown in sight.[1] Driven by a mix of forces ranging from digital transformation to mobile devices to IoT, this explosive growth in identities brings with it an increased risk of identity-related breaches. And these breaches can occur on many fronts — not just via phishing attacks, but social engineering schemes, brute force attacks, and more.

In this report, sponsored by the Identity Defined Security Alliance (IDSA), we examine the risks endangering enterprise identities and explore why some companies are doing better at securing those identities than others. Based on an online survey of security and identity professionals in the U.S. with more than 1,000 employees, the study investigates the benefits, challenges, and progress of enterprise efforts to adopt an identity-centric approach to security.

Key Findings

- **Identity-related breaches are ubiquitous**
  - 94% have had an identity-related breach
  - 79% have had an identity-related breach within the past two years
  - 66% say phishing is the most common cause of identity-related breaches
  - 99% believe their identity-related breaches were preventable
- **Identity security is a work in progress**
  - Most identity-related security outcomes are still in progress or planning stages
  - Less than half have fully implemented key identity-related security outcomes
  - 71% have made organizational changes to the ownership of identity management
- **Forward-thinking companies are showing results**
  - Companies are much more likely to have fully implemented key identity-related security outcomes
  - Only 34% of companies with a "forward-thinking" security culture have had an identity-related breach in the past year — far fewer than the 59% of companies with a "reactive" security culture

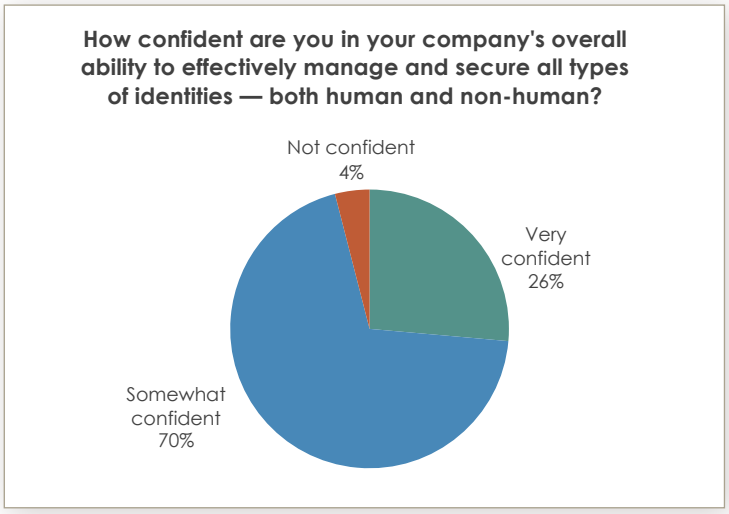
[1] December, 2019. *The State of Identity: How Security Teams are Addressing Risk*

Detailed Findings: Identity-related breaches are ubiquitous

There is widespread lack of confidence in the ability to effectively secure identities

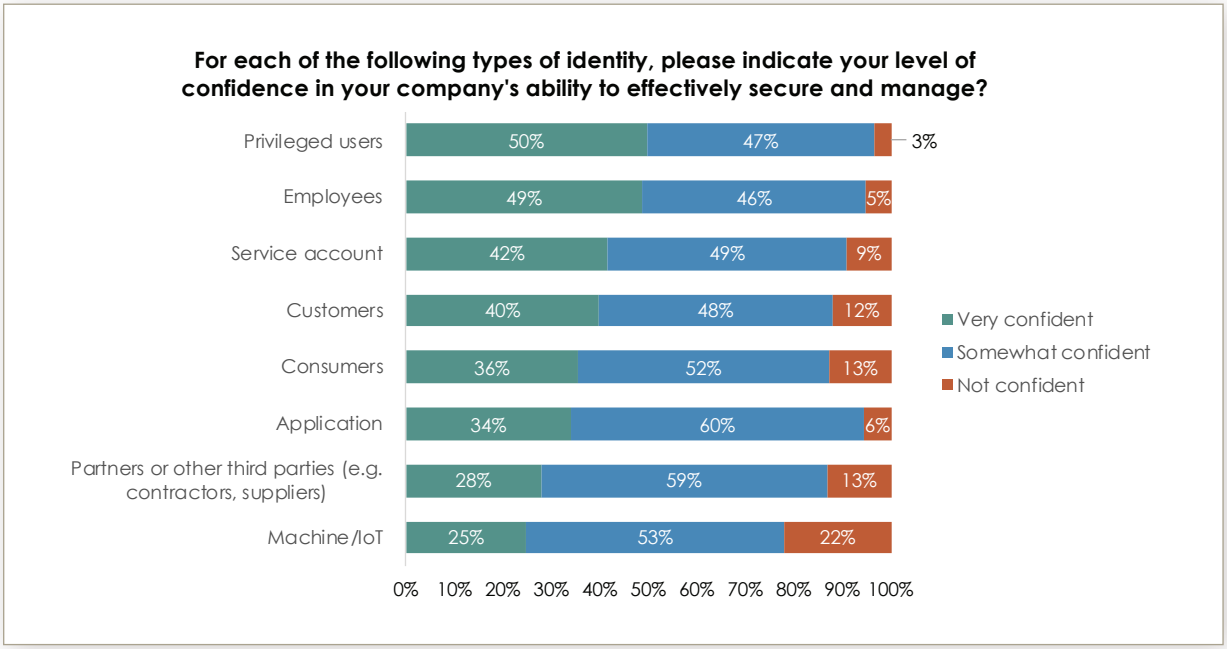
To a cyber attacker, the right identity is extremely valuable. It can be used to break into a network, move laterally once inside, and facilitate all manner of fraud and identity theft. Whether it is by phishing or some other means, obtaining stolen credentials is often a critical part of a threat actor's agenda. For this reason, protecting identities must be a crucial part of any security strategy. Yet while security is top of mind for most enterprises, many lack confidence in their ability to completely protect identities despite knowing what's at stake.

To decipher current trust levels at large companies, we asked IT security and identity professionals about their confidence in their company's overall ability to effectively manage and secure all types of identities. Nearly three-quarters (74%) say they are somewhat or not confident, and only a quarter (26%) report they are very confident when considering the entire threat attack surface.



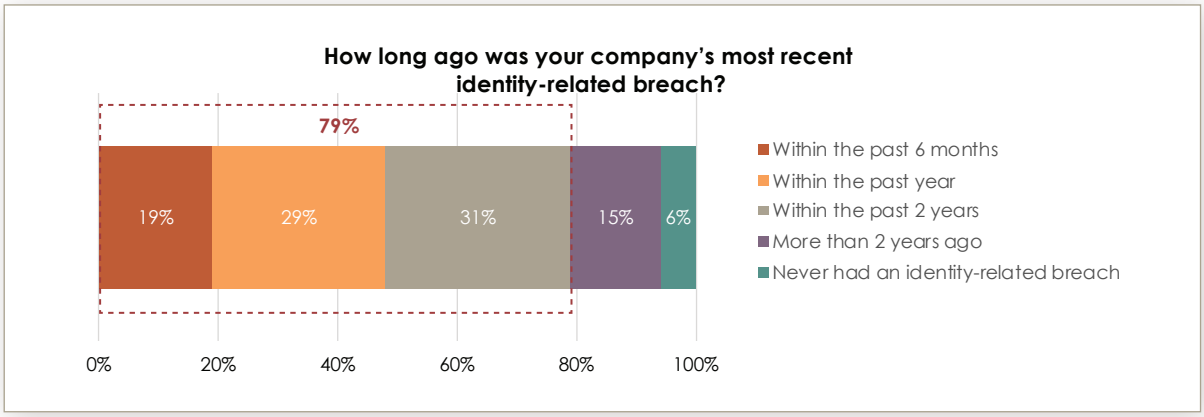
In order to add color to this finding, we drilled down further on the responses by different types of identities — both human and non-human. Confidence levels were lowest for machine/IoT and partners and highest for privileged users and employees. It is not surprising that privileged users are at the top of the list since they carry significantly more risk and additional attention is given to these important credentials. However, it is worrisome that even these most important identities still have only half (50%) reporting a high level of confidence.

Since security in any environment is only as strong as the weakest link, it is not surprising that the "very confident" responses across specific types of identities were all notably higher than the 26% reported in the general question above, with the single exception of machine/IoT.



Most companies experienced an identity-related breach within the past two years

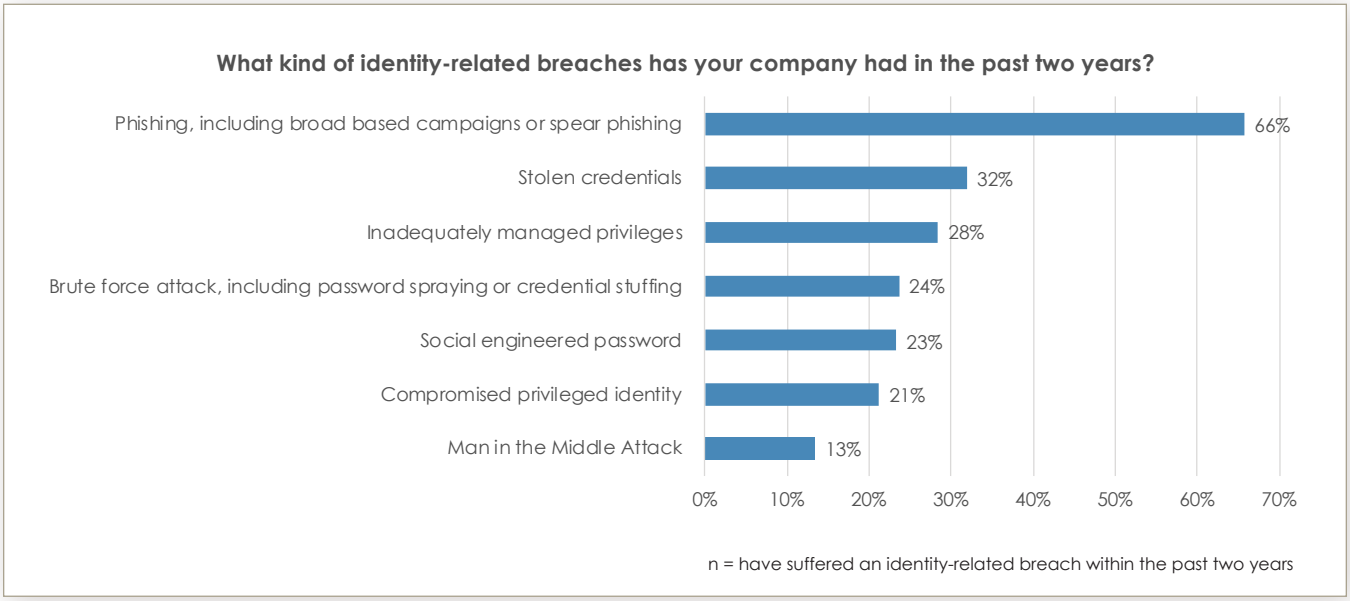
One of the reasons for this lack of confidence among security and identity professionals may be their own first-hand experiences with breaches. The vast majority of IT security and identity professionals (94%) have experienced an identity-related breach within their organization at some point. Even more disconcerting is that 79% of security professionals say they have had a breach at their company within the past two years.



Phishing is by far the most common cause of identity-related breaches

To make sense of an identity-related breach headline in the news or analyze an incident in your organization, it helps to understand the different attack vectors a cyber criminal might try to cause potential damage. Given that the security landscape is rapidly changing, this study focuses specifically on breaches in the past two years.

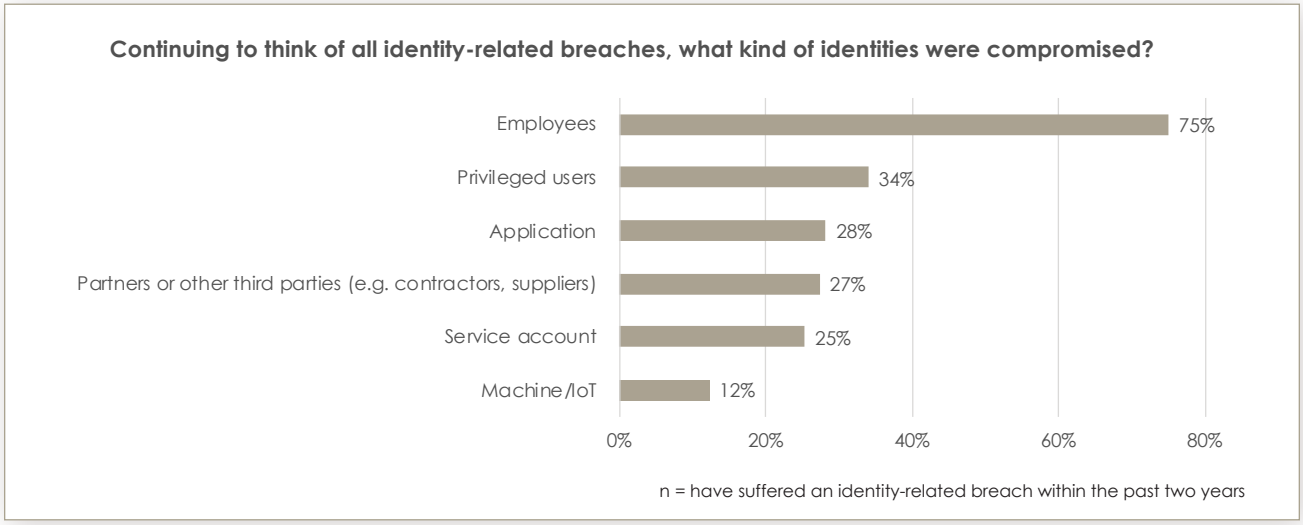
Security and identity professionals consistently report that within the last two years, by far, the number one cited cause of identity-related breaches was phishing (66%). This included both broad-based campaigns and more targeted spear phishing. While phishing was the most common cause of breach identified, there are a wide range of others including stolen credentials (32%), inadequately managed privileges (28%), brute force attacks (24%), social engineered passwords (23%), and more.



While it's important to recognize the leading types of current breaches, it is equally critical to consider all types of identities that need to be protected when developing a security strategy.

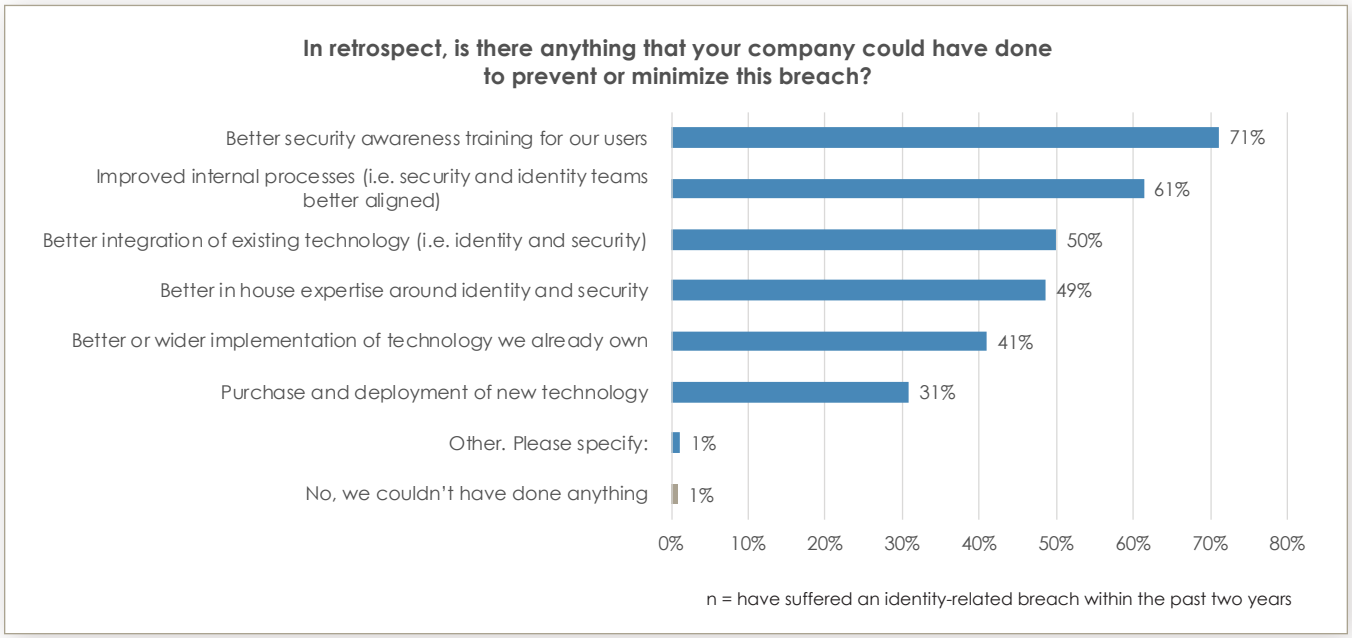
In today's enterprise, there are two primary categories of workforce identities: humans (e.g., employees, privileged users, partners) and non-humans (e.g., applications, service accounts, machines/IoT). Humans utilize usernames and passwords to identify themselves. Similarly, non-humans also need to identify and authenticate themselves when they connect to each other. However, non-humans use keys and certificates instead of usernames and passwords. Regardless of the type of identity, all can be attacked if not adequately protected.

When asked about the types of identities more likely to be involved in breaches, human identities top the list with 75% of security and identity professionals disclosing compromised employee identities followed by privileged users (34%), and partner or other third parties (27%). On the opposite end, non-human identities — machines/IoT (12%), service accounts (25%), and applications (28%) are less likely to be compromised in a breach.



Almost everybody believes identity-related breaches were preventable

One of the key revelations of this study is that almost all (99%) of security and identity professionals believe the identity-related breaches at their company were preventable. Participants reported that better security awareness training for users (71%), improved internal process (61%), better integration of existing technology (50%), better inhouse expertise around identity and security (49%), better or wider implementation of technology already owned (41%), and the purchase and deployment of new technology (31%) could all have saved their companies from a breach in the past two years. A few individuals also took the time to write in "other" responses, including specific types of training, multi-factor authentication (MFA), and higher-level management approval to enable technologies.



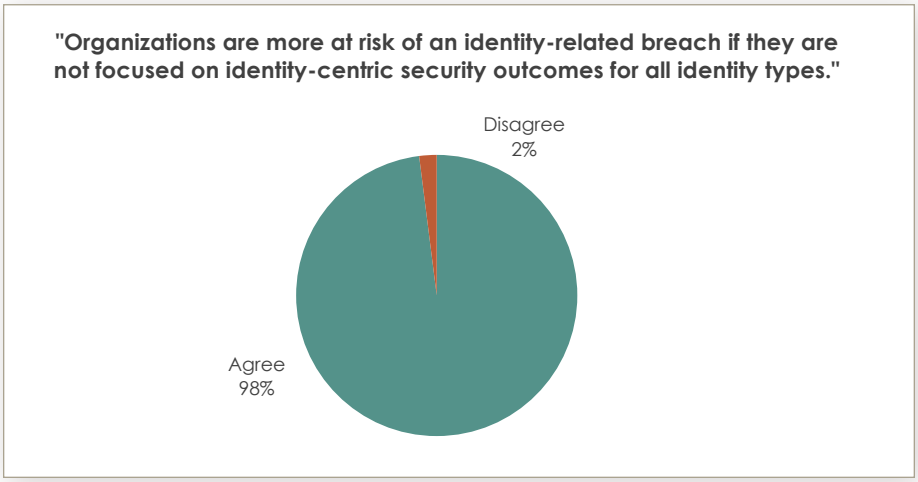
Every security stakeholder should take a moment to reflect on this data: *participants most frequently cited training as the way to prevent identity breaches*. Is depending on users to do the right thing really the most effective solution? Even though employees can be trained to better safeguard their work identities and tested using simulated phishing exercises, they are still human and not without fault. In addition, cyber criminals are staying one step ahead and constantly improving their methods of tricking users into revealing passwords or unintentionally installing malicious code. There may be a more optimal approach for improving identity security — perhaps not just training and testing, but implementing technology solutions. For example, companies could deploy solutions to automatically detect the inappropriate use of valid credentials and prevent access based on device characteristics or user behavior, or implement multi-factor authentication for all users.

Detailed Findings: Identity security is a work in progress

Most identity-related security outcomes are still in progress or planning stages

Today's work environment bears hardly any resemblance to that of several decades ago. Mobile technology has become ubiquitous in business environments, enabling employees and partners to communicate and collaborate in unexpected ways. Cloud services are commonly used to give companies more flexibility, additional features, and less maintenance, often at reduced costs. However, these changes have fundamentally altered the attack surface security professionals need to protect, which is creating a race to secure the enterprise at the speed of change.

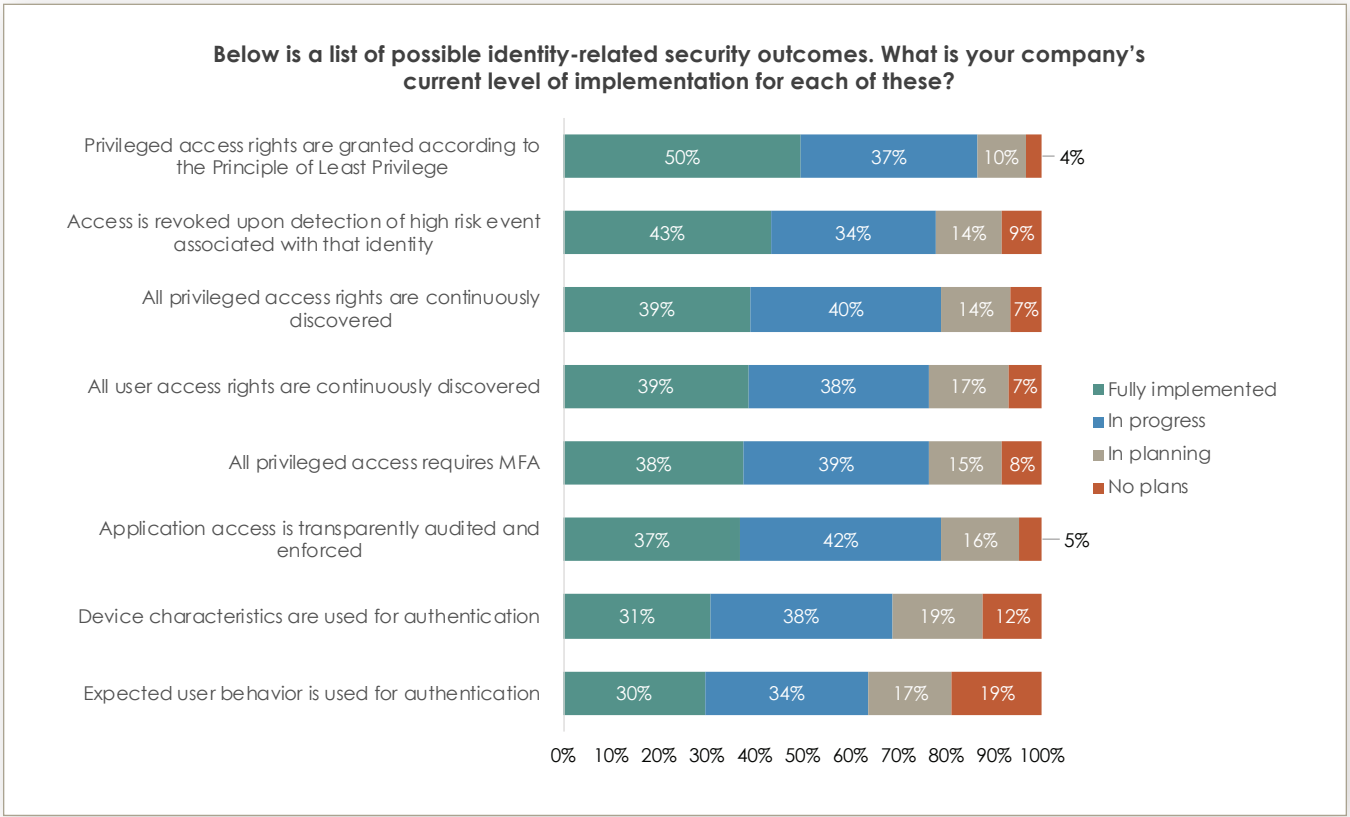
As our work world continuously evolves, so must the security to protect important workforce identity assets. As such, it's constant work in progress for security professionals as nothing is ever "done" in the enterprise. Yet it's often hard to predict what's behind the next turn, and be able to focus the right attention, when this environment is in constant flux. Security and identity professionals couldn't agree more. Almost all (98%) believe that a lack of focus on identity-centric security outcomes for all identity types increases their risk of breach.



When considering what's at stake, security professionals must first consider a range of desired outcomes, or results, they want to achieve and then chart their paths accordingly. To understand the real-life enterprise experiences from those in the trenches combating cyber attackers, we asked about their progress with key identity-related security outcomes recommended by the IDSA. *See https://securityoutcomes.idsalliance.org for more detail.*

According to security and identity professionals, these outcomes are predominantly still a work in progress or in the planning stages for most companies. On the downside, less than half report that they have fully implemented any of the key identity-related security outcomes investigated in this study. On the positive side, most companies are actively trying to do better and have identified these outcomes and are working on implementation, even if they are only in the planning stage.

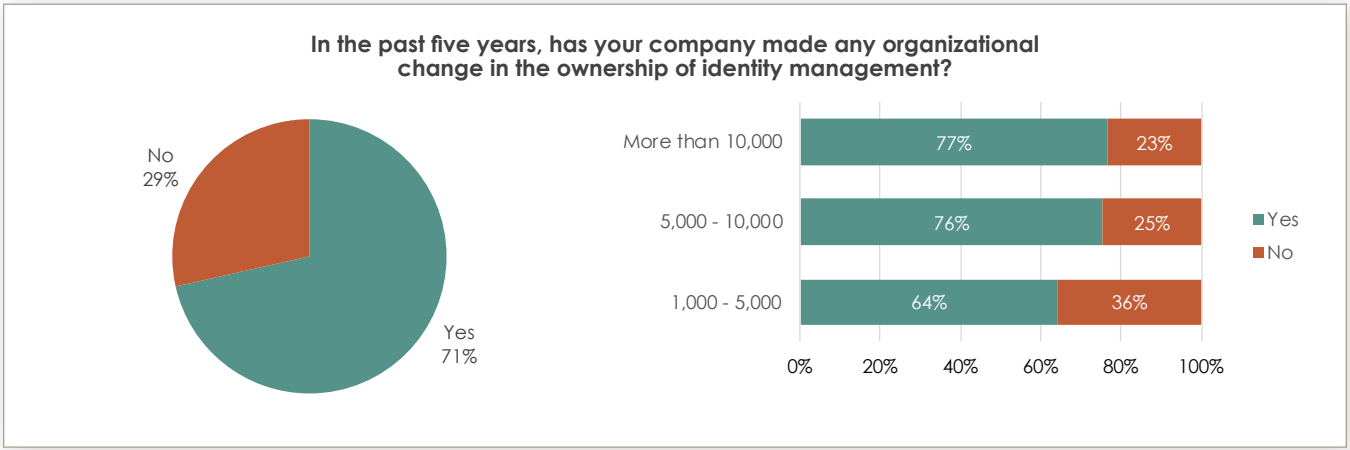
Definition: For this survey, an "identity-defined security outcome" is a desired result that improves an organization's security posture through identity-centric security and reduces the risk of a breach or failed audit. *Source: IDSA*



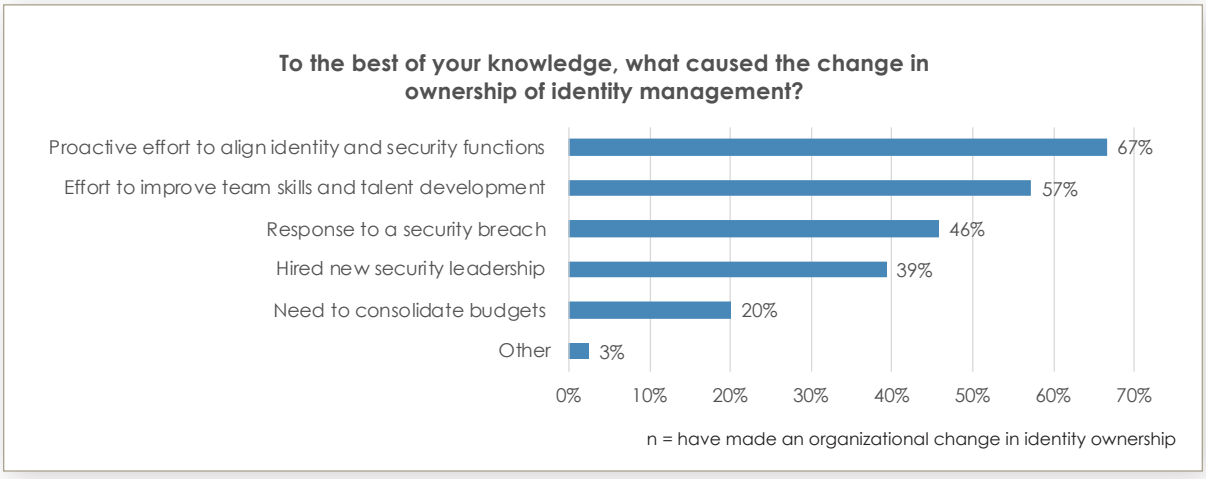
Given the high number of breaches caused by phishing attacks, it should be noted that two of these outcomes can greatly reduce that risk — expected user behavior for authentication and device characteristics for authentication. Yet they are the areas where security teams are the least mature. Both of these outcomes are risk-based authentication mechanisms, which grant users access to resources only if certain device or behavioral data indicates that the users are actually who they say they are. These two outcomes, along with the implementation of MFA for all users (not just for privileged users), could help prevent the use of credentials stolen through phishing mechanisms.

Companies are making organizational changes to improve identity security

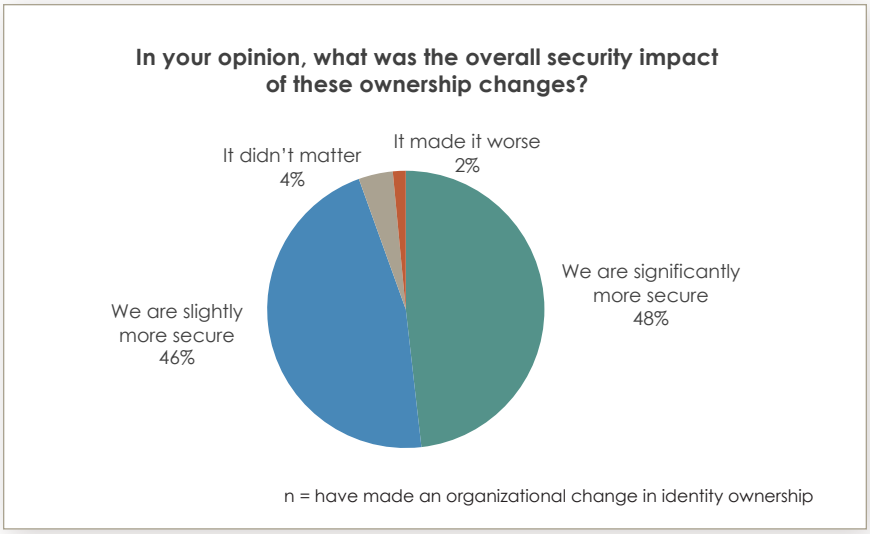
A fundamental way enterprises can effectively manage identities and reduce risk is through effective organizational changes that ensure the expertise of both the security and identity teams are fully leveraged. In an earlier study, we reported a notable difference in identity strategy awareness among security teams assuming leadership in IAM. This current study further explores this trend by asking security and identity professionals about their organizational changes related to identity management. A majority (71%) have made organizational changes to the ownership of identity management in the past five years. This number jumps to over three-quarters in companies with 5,000 employees or more.



Of particular importance are the factors prompting these management changes. According to security and identity professionals, the two leading causes for a change in ownership are proactive, including efforts to align identity and security functions (67%) and improvements made in team skills and talent development (57%). Still, almost half (46%) required the painful consequence of a breach to cause these leadership changes. Notably, a few "other" responses submitted by survey participants were overall IT restructuring, loss of staffing, regulations, and the creation of a security committee.



In reviewing these leadership shifts, were they viewed as simply change for change's sake or did they generate significant improvements in safeguarding the organization from potential intruders? Overall, recent ownership changes were consistently described as good for security, with close to half (48%) saying they are significantly more secure and 46% saying they are slightly more secure. Only a handful of organizations reported that it didn't matter (4%) or made it worse (2%).

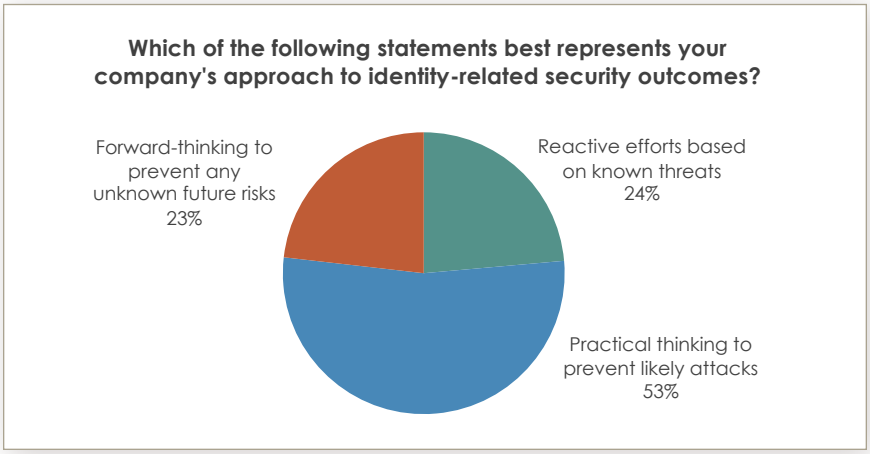


Detailed Findings: Forward-thinking companies are showing results

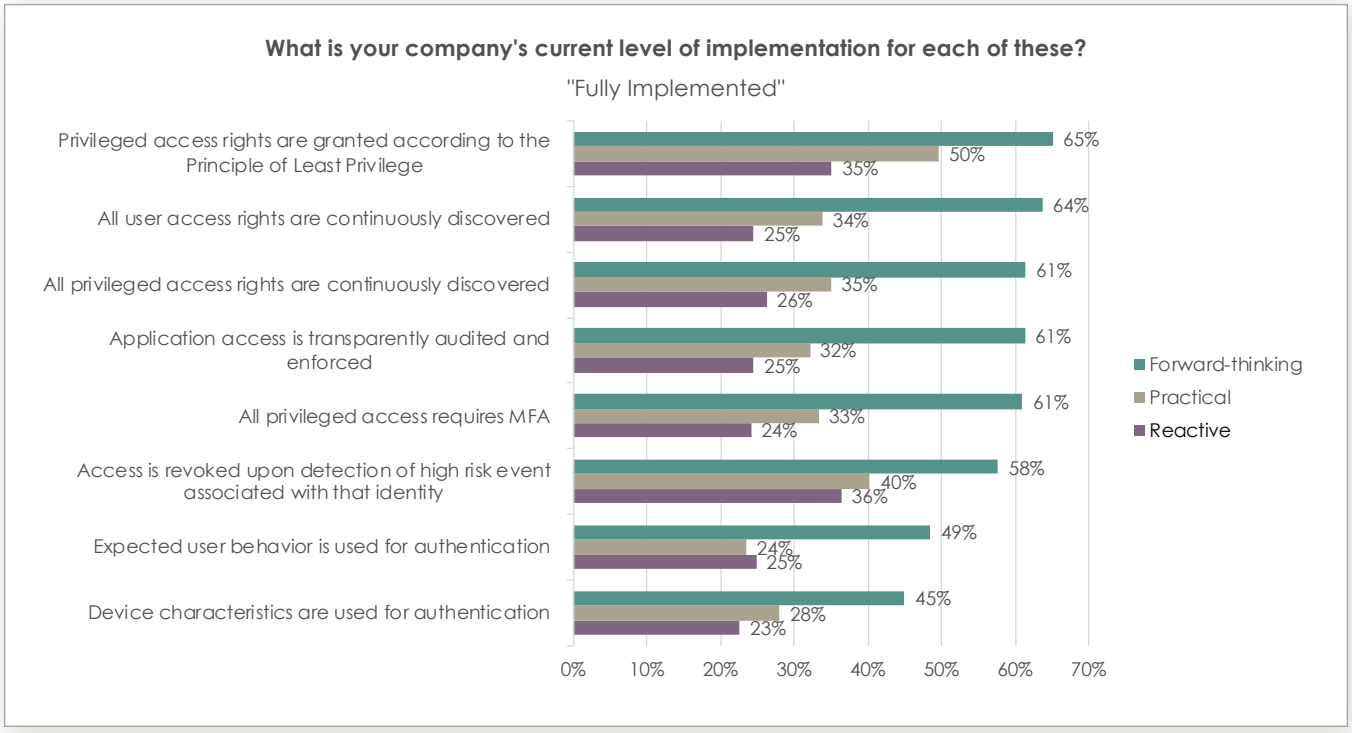
Forward-thinking companies are far more likely to have fully implemented security outcomes

As clearly outlined above, identity security is a work in progress. One of the goals of this study was to determine if a focus on identity-centric security strategies impacted the overall security posture of the organization. We explored this idea by comparing levels of maturity — both self-described and progress on security outcomes — with incidents of security breaches. This analysis shows a clear correlation between a focus on identity-centric security outcomes and lower numbers of breaches.

When asked to self-describe the maturity of their identity-related security outcomes, there are three distinct buckets among security professionals. Almost a quarter (23%) characterize themselves as "forward-thinking." Conversely, almost a quarter (24%) are "reactive" focusing their efforts on known threats and about half (53%) of companies are applying "practical" thinking to avert the most likely attacks.



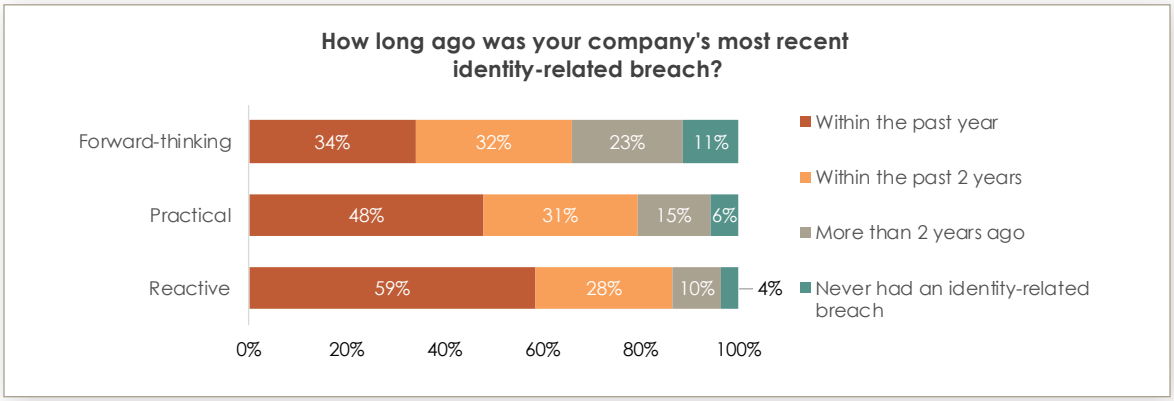
It is especially noteworthy that "forward-thinking" companies are genuinely doing a better job. They are not just patting themselves on the back, their progress toward full implementation of key security outcomes is notably higher. When we compare implementation levels in "forward-thinking" organizations with those using more reactive approaches, the forward thinkers are significantly further ahead.



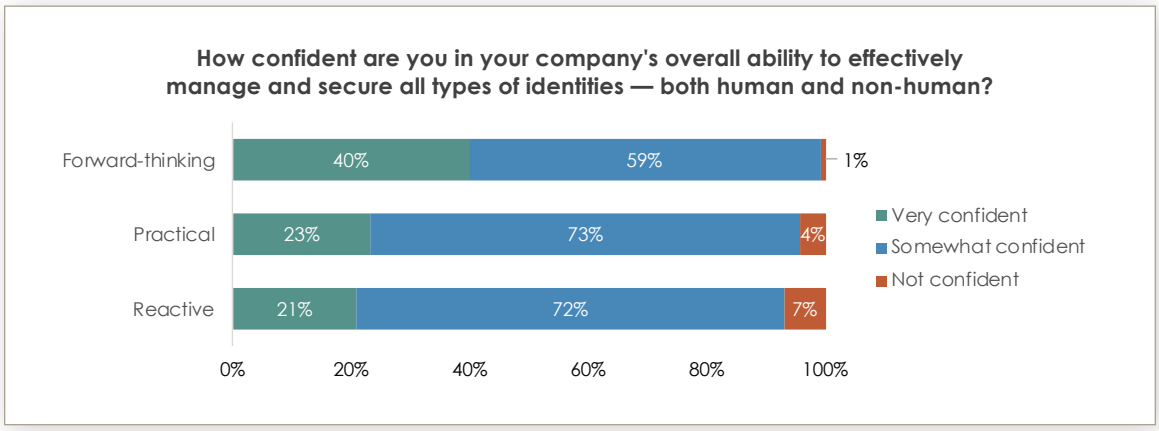
Forward-thinking companies have significantly fewer identity-related breaches

The most important takeaway from the research is that not only are forward-thinking organizations further ahead in full implementation of security outcomes, they are also experiencing fewer identity-related breaches!

Only a third (34%) of companies with "forward-thinking" approaches to identity security experienced a breach in the last year. This is far fewer than the 59% of companies with "reactive" security approaches. They also out-performed companies with "practical" approaches (48%).

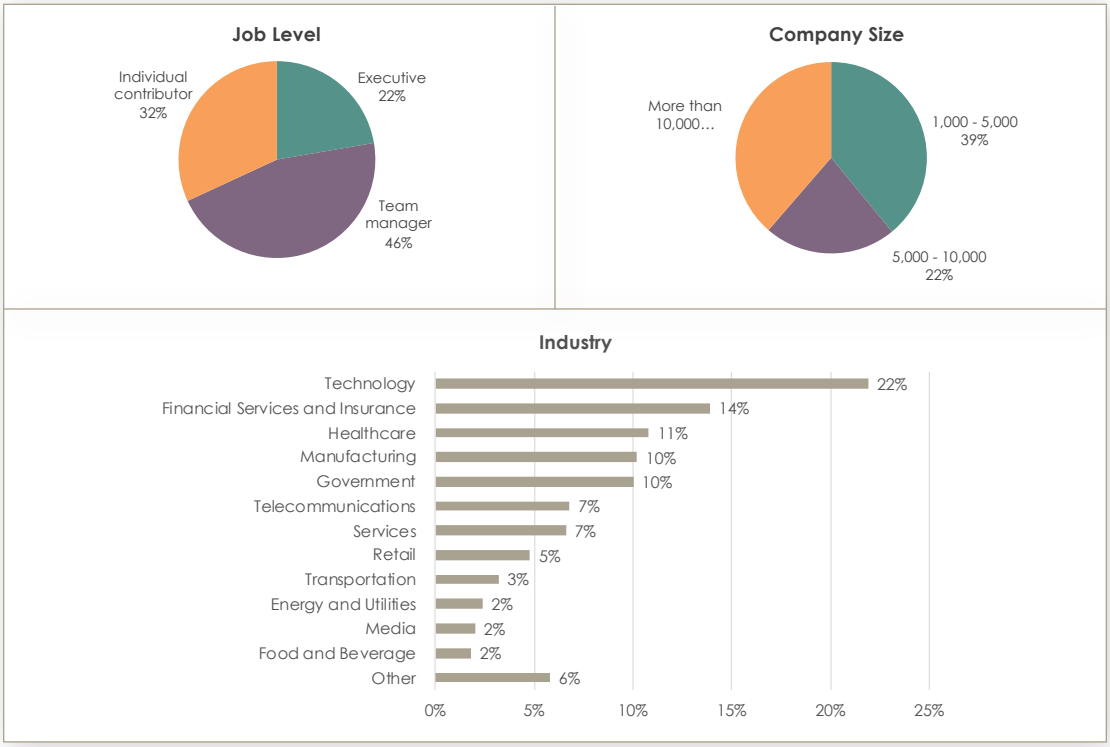


Forward-thinking prepares enterprises to not only avoid pitfalls and failure, but to also build confidence that helps foster success. With more planned efforts in effectively managing and securing identities, organizations can begin growing their confidence levels and, ultimately, work towards reducing risk. The data clearly demonstrates this. Almost twice as many (40%) stakeholders at "forward-thinking" companies said they are very confident in their company's overall ability to effectively manage and secure all types of identities than those at companies who have a "reactive" approach (21%).



Survey Methodology and Participant Demographics

In April 2020, an online survey was sent to an independent database of security and identity professionals in the United States. A total of 502 qualified individuals completed the survey. All participants were directly responsible for IT security or IAM at companies with more than 1,000 employees. Participants included a mix of job levels, company sizes, and industries.



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. For more information visit www.idsalliance.org.