IDENTITY DEFINED SECURITY ALLIANCE

dimensional research

2023

Trends in Identity Security

A Survey of IT Security and Identity Professionals

Research

idsalliance.org

Table of Contents

Introduction

Protecting digital identities has never been more crucial as cyber-attacks rapidly increase in sophistication and volume. Organizations need to ensure only the right people have access to the right data, networks, and systems and use technologies that prevent malicious actors from gaining access to sensitive information.

To explore the current state of cybersecurity, we commissioned a study with Dimensional Research to understand the approaches large companies are taking toward security and identity. The study invited independent security and identity professionals across the United States, who were asked a range of questions focused on their current plans, identity and security history, and more. The survey was completed by 529 qualified individuals with deep knowledge of IT security and identity from organizations with more than 1,000 employees.

The research finds that as the number of identities increases, more businesses are suffering identity-related incidents and are identifying securing them as a critical priority. However, we also discover that securing these identities remains a significant challenge, and security outcomes remain a work in progress.

We'll begin by exploring the current state of identity and security before digging into some of the security challenges and necessary outcomes.

Highlights

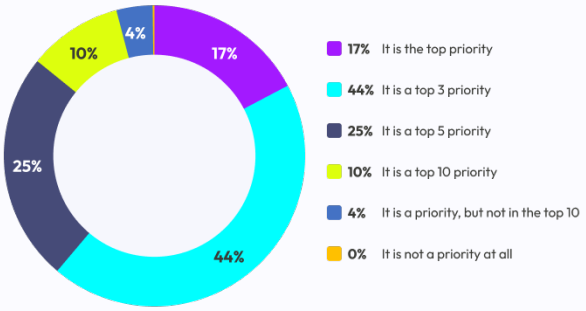
- Multiple factors driving an increase in the number of identities
- Only half (**49%**) report their company leadership proactively invests in securing identities
- Wide range of identity-related use cases identified for artificial intelligence and machine learning
- Identity-related incidents have direct business impact

The State of Identity and Security in 2023

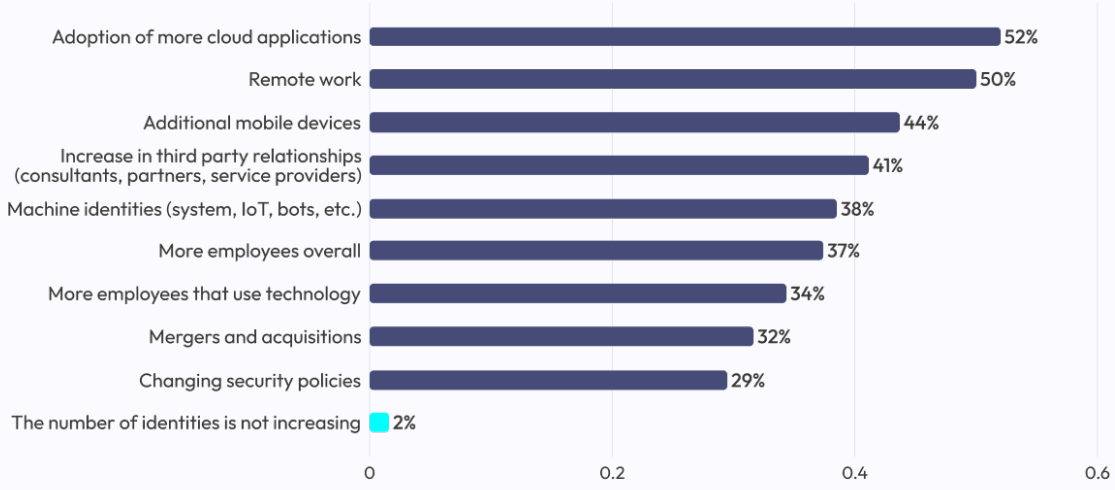
Our research found that 17% of businesses now see managing and securing digital identities as the number one priority of their security program, up from 16% in 2022. More than two-fifths of respondents (44%) said they now see it as a top three priority, and another quarter (25%) see security digital identity as a top five priority. Only 4% of businesses don't see securing identities as a top 10 priority.

The focus on security digital identities is not surprising given the growth across identity types. The critical factors driving this growth were identified as the growing adoption of cloud applications (52%), the rise of remote working (50%), more mobile device usage (44%), and more third-party relationships (41%)

How would you characterize the importance of effectively managing and securing digital identities within your company's security program?
Choose the one answer that most closely applies.



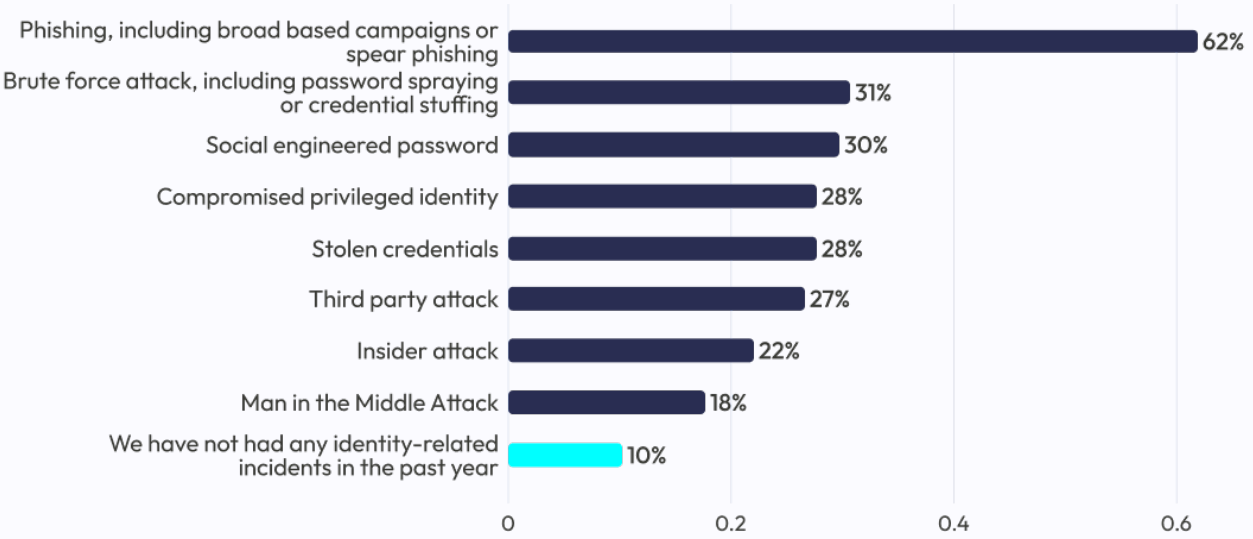
What factors are driving an increase in the number of identities at your company?
Choose all that apply.



With this spike in digital identities comes an increase in cyber-attacks targeting them. By far the most significant reason behind this was phishing (62%). Among these companies that suffered a phishing attack, the most typical trajectory was email phishing (93%), while 49% had suffered a spear phishing attack, and 27% had been victims of vishing or smishing incidents. Other types of identity-related incidents included brute force attack (31%), social engineered password (30%), compromised privileged identity (28%), stolen credentials (28%) and more.

What kind of identity-related incidents has your company had in the past year?

Choose all that apply.

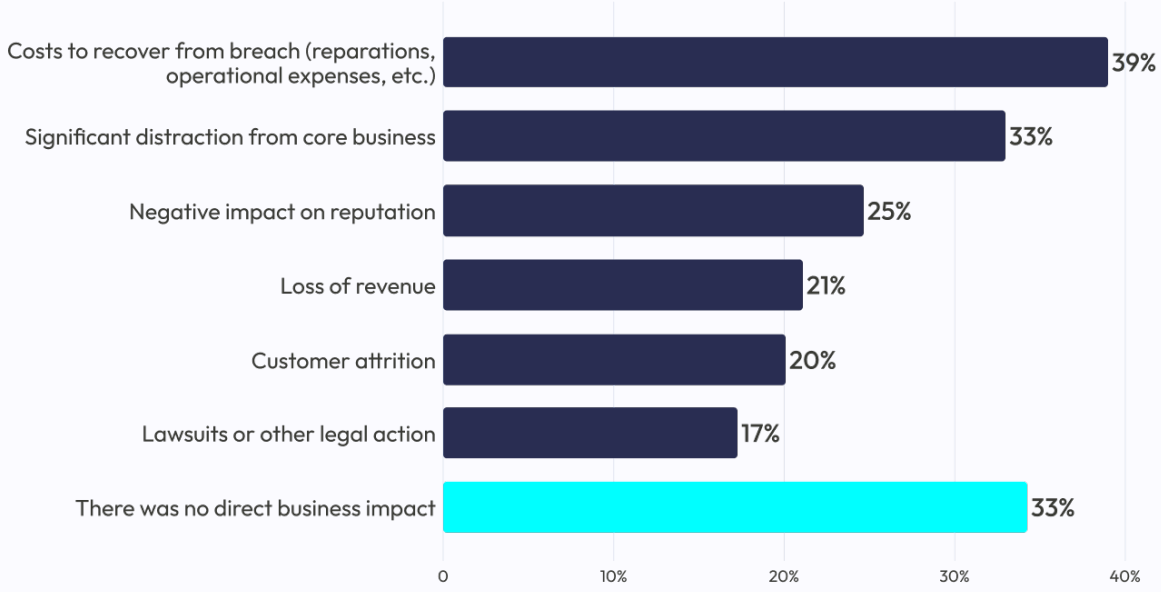


Employee behavior is often the cause of identity-related incidents. In line with the above data, clicking on a phishing email is the most common (57%). Also reported as a cause of an incident were employees using the same passwords for work and personal accounts (37%), followed by hackers using social engineering techniques, employees using non-authorized devices, and users sharing credentials with their colleagues (all 31%).

68% of identity stakeholders said these attacks directly impacted their business. The most significant impact was the cost of recovering from the breach (39%), followed by distracting from core business (33%) and the negative impact on the company's reputation (25%).

Did your company suffer any direct impact to business results as a result of identity-related incidents in the past year?

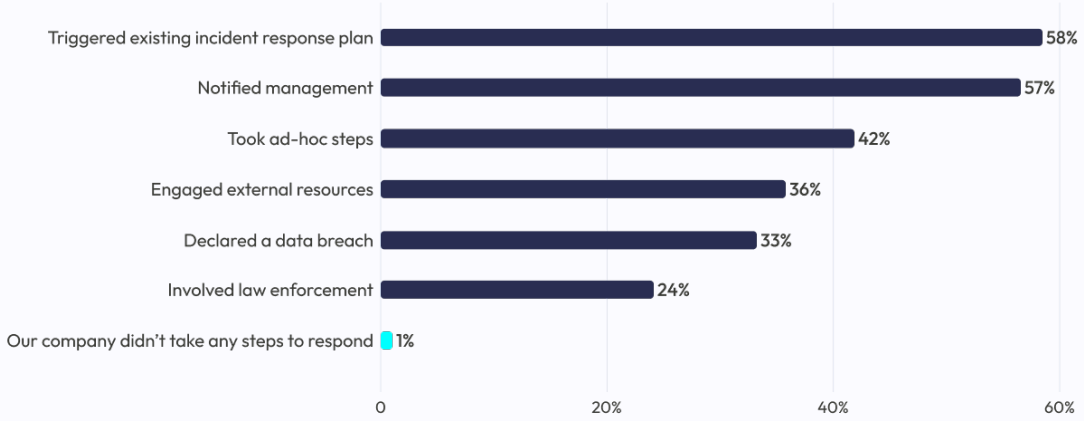
Choose all that apply.



How businesses respond to attacks is critical to preventing data loss and minimizing the effect of the incident. The research found that only one in three businesses' identity and security teams (33%) declared a data breach, and less than a quarter (24%) involved law enforcement. The most typical responses to an incident included 58% of the teams triggered their existing incident response plan, and 57% notified their management team.

What actions did your company's identity or security teams take in response to these identity-related incidents?

Choose all that apply.



Ongoing Challenges of Identity Security

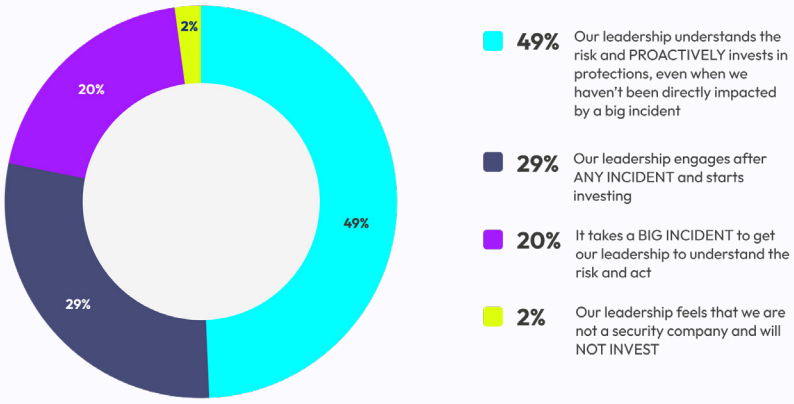
Our research found that one of the biggest challenges for security teams was the sheer number of barriers they now face. The top two reasons were identity frameworks being complicated by multiple vendors and different architectures (40%) and complex technology environments (39%). While respondents also identified insufficient budget (30%), a lack of expertise (29%), standards (26%), people (25%), and governance (23%).

What barriers prevent your company from doing more to secure identities?

Choose all that apply.

A significant reason these barriers hold companies back appears to be a lack of proactive investment from senior leadership. Just under half of the identity stakeholders (49%) said that their leadership teams understand identity and security risks and proactively invest in protection before they've suffered an incident. Well over a quarter of leadership teams (29%) begin to engage and support after an incident, and one in five (20%) will only take action after a major incident.

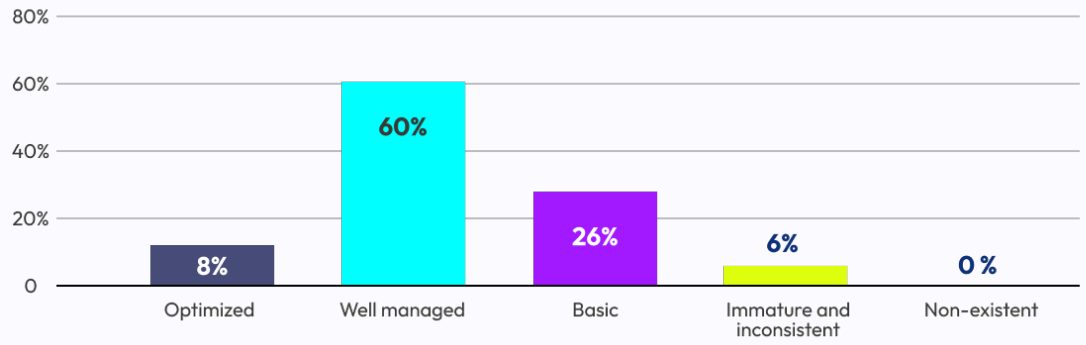
Which of the following statements best represents your opinion of how your company leadership prioritizes investments in securing identities?



The majority of identity stakeholders (60%) said their company's security identity capabilities were well managed, and only 8% said they were optimal. While one quarter (26%) only believe their company has basic security identity capabilities.

How would you personally characterize your company's capabilities for securing identities?

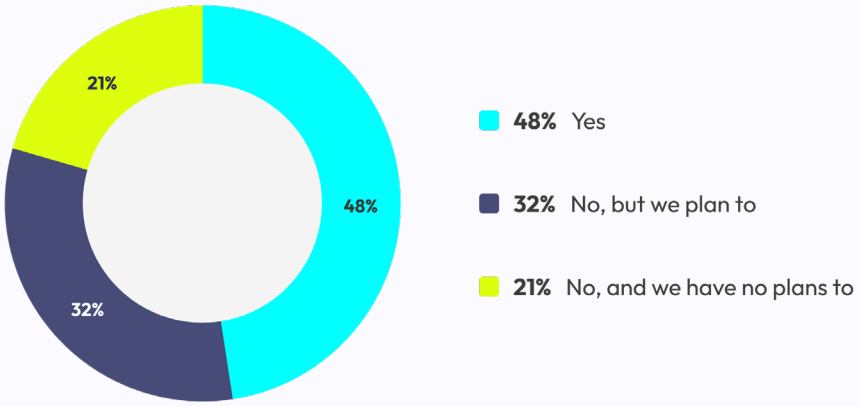
Choose the one answer that most closely applies.



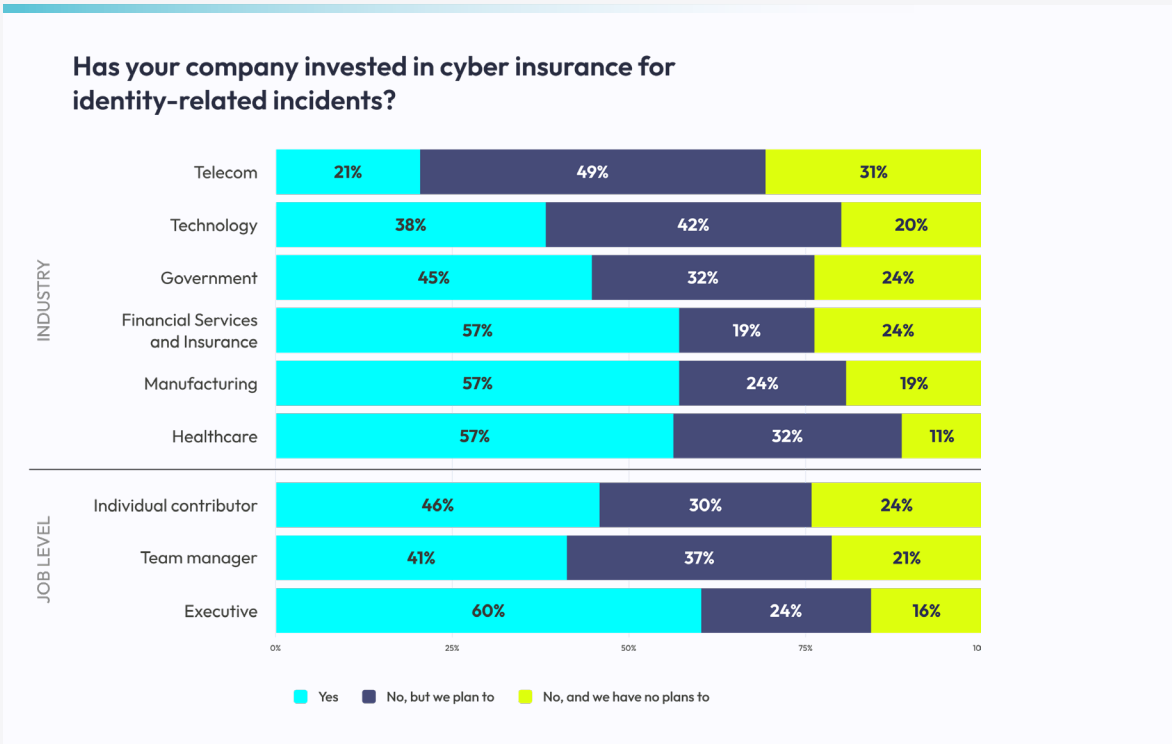
How 2023 Trends Are Impacting Identity Security

The study found that the majority of businesses (89%) are somewhat or very concerned that new privacy regulations will impact their identity security. This may be why cyber insurance for identity-related incidents is becoming increasingly common, with 48% of businesses having already invested and 32% planning to.

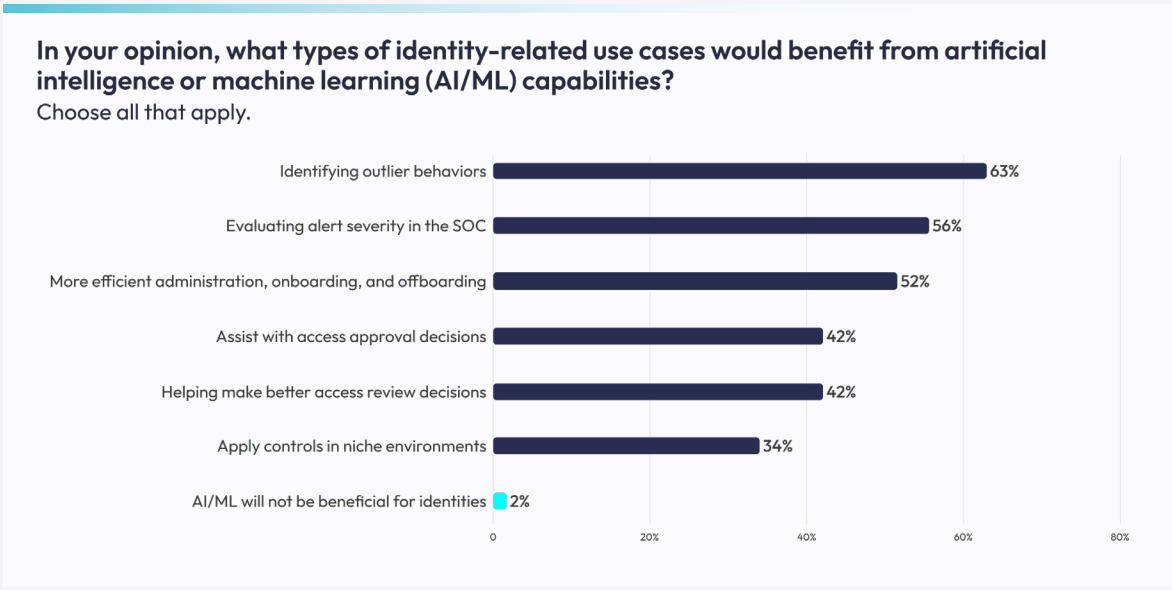
Has your company invested in cyber insurance for identity-related incidents?



This cyber-insurance trend is most common in highly-regulated industries, with 57% of businesses in the healthcare, manufacturing, and financial services sectors having already invested. It is also interesting to note that executives are much more likely to report that their company is making these investments, with 60% already investing in cyber insurance for identity-related industries.

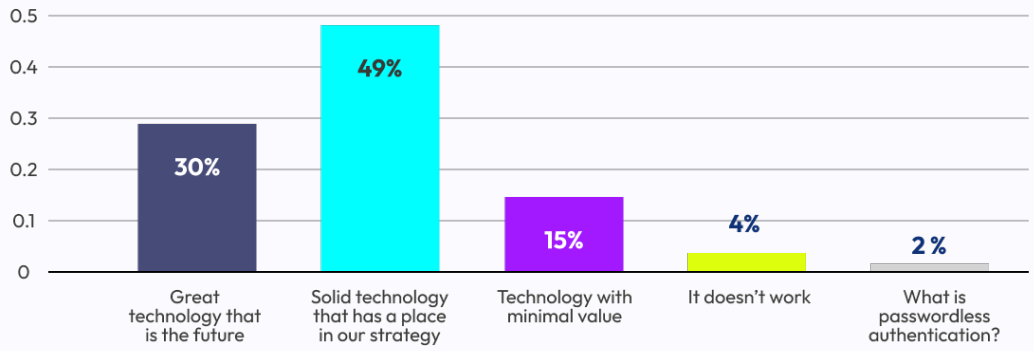


The research also explored the technologies that are required to address identity security challenges. For example, respondents were asked about the use cases they perceived as having the most benefit from artificial intelligence and machine learning. Identity and security stakeholders consistently (98%) report AI/ML will be beneficial. The number one use case was identifying outlier behaviors (63%), followed by evaluating the severity of alerts (56%), and making administrative tasks more efficient (52%).

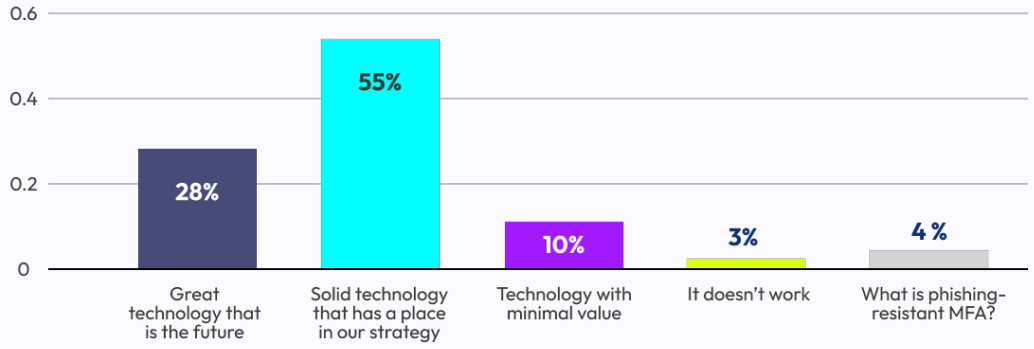


Identity stakeholders see passwordless authentication as a tool in addressing identity issues, with 79% saying it's a great or solid technology. Respondents were also optimistic about phishing-resistant multi-factor authentication (MFA), with 83% saying it's a great or solid technology for the future. Social media is also a key concern for businesses, with 90% saying they were slightly or very worried about employees using corporate credentials for their social media accounts.

What is your opinion of passwordless authentication?



What is your opinion of phishing-resistant MFA?



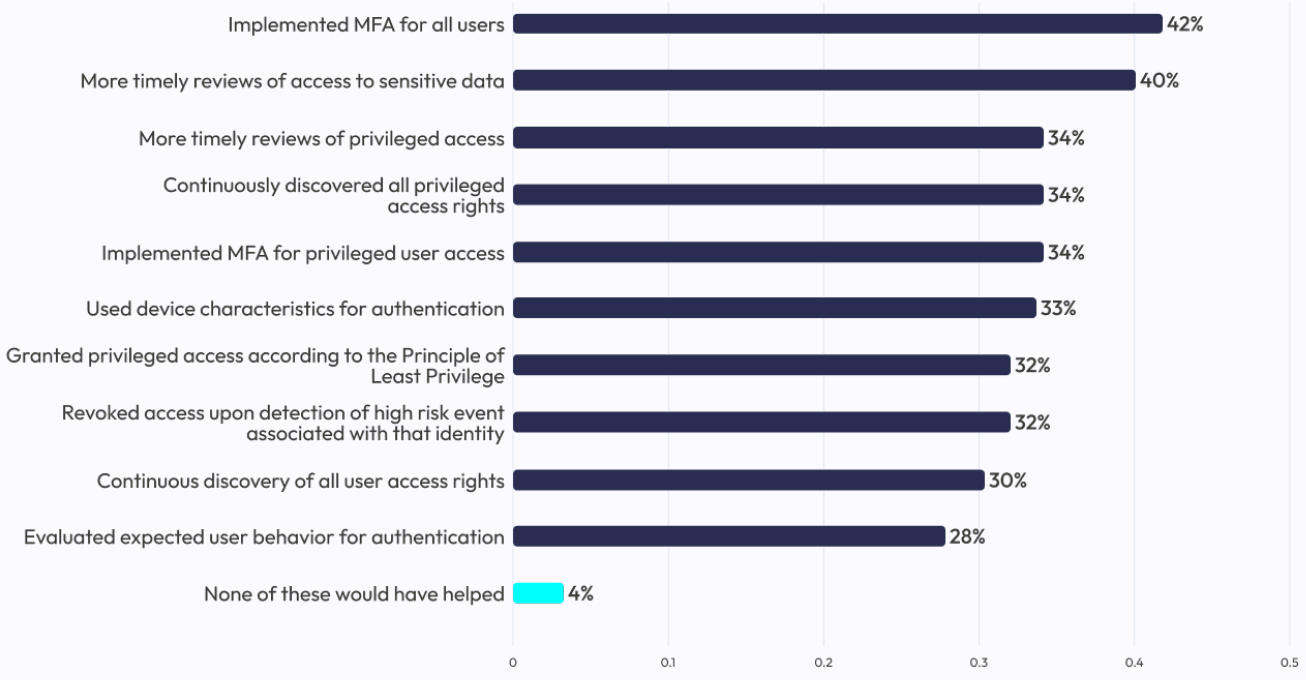
Security Outcomes Remain A Work In Progress

Identity stakeholders also provided insight into their company's level of implementation of identity-related security outcomes. The most advanced outcome was privileged user access, with 58% of companies fully implementing it and 26% saying it was in progress.

Additionally, 96% of identity stakeholders said that security outcomes could have lessened the business impact of incidents. For example, 42% of respondents said implementing MFA for all users could have prevented or minimized the effect of incidents, followed by timely reviews of access to sensitive data (40%) and privileged access (34%). The research also found that identity stakeholders identified using authentication and discovering user access rights and behavior as critical to addressing identity threats.

In retrospect, could any of the following have prevented or minimized the business impact of the incident?

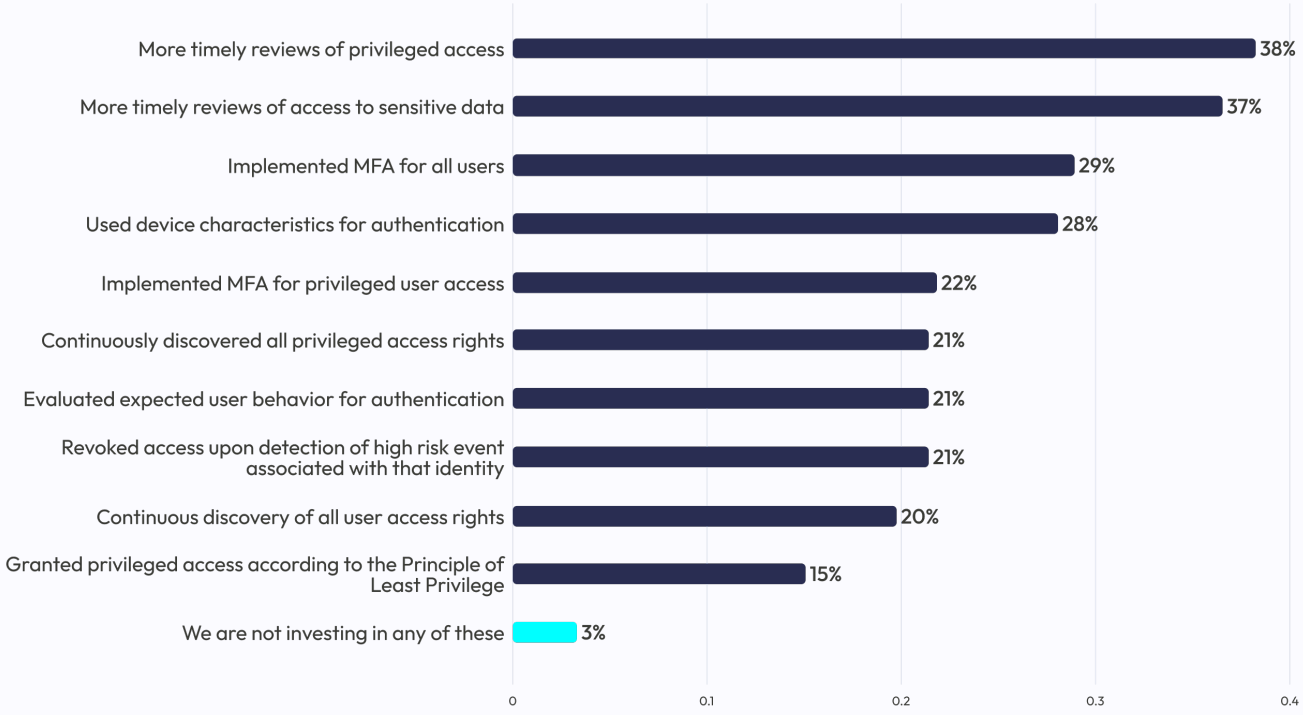
Choose all that apply.



97% of businesses plan to further invest in security outcomes in the next 12 months. Top of the list is ensuring more timely reviews of privileged access (38%) and access to sensitive data (37%). Businesses are also increasing investment in MFA for all users (29%) and user device characteristics for authentication (28%).

Which of the following is your company investing the MOST in over the coming year?

Choose up to three of the following.



Prioritize Securing Identities With IDSA

Securing digital identities is a critical priority for organizations across all sectors in the fight against ever-evolving and increasingly sophisticated cyber threats. Our research finds that businesses recognize the risk of identity-related incidents and increasingly prioritize the dangers in their security programs.

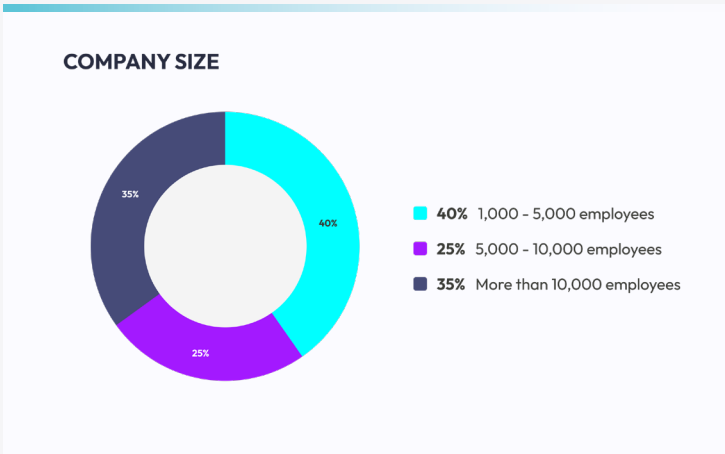
It's clear that more involvement and investment from senior leadership teams are required to help businesses address these threats. Companies must also address the complexity of their systems and technology architectures and gain access to security expertise and standards to help them better manage their risk. To do that, security teams need to ensure they have the right processes, tools, technologies, and communication to discover and mitigate identity security threats as quickly as possible.

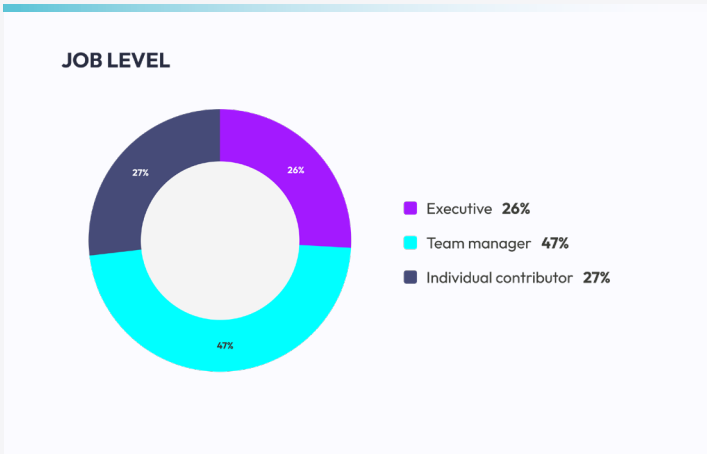
Goals & Methodology

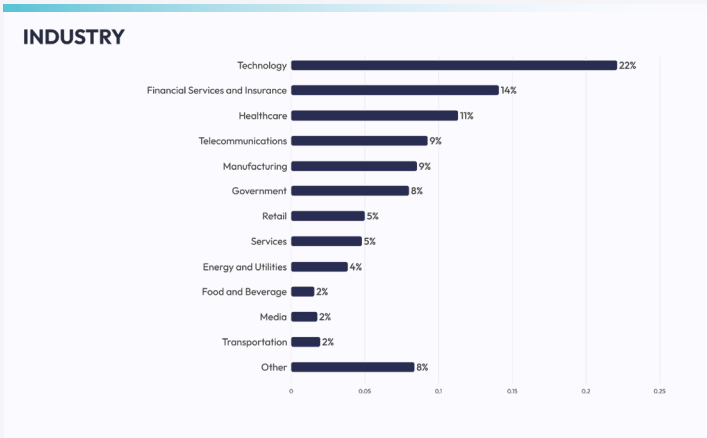
The primary research goal was to understand the experiences and approaches towards security and identities at large companies.

Independent sources of security and identity professionals in the United States were invited to participate in an online survey. A variety of questions were asked on history with identities and security, current plans, and other topics. Certain questions were repeated from similar surveys conducted in 2021 and 2022 to enable trend analysis.

A total of **529 qualified individuals** completed the survey. All were directly responsible for IT security or identities at a company with more than 1,000 employees and were very knowledgeable about both IT security and identities.







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 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 on the Identity Security Alliance and how to become a member, visit **www.idsalliance.org**.