
# 2022 Trends in Securing Digital Identities

Research

dimensional research

IDENTITY DEFINED
SECURITY ALLIANCE

# Table of Contents

# Introduction

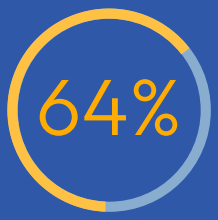
Managing the ecosystem of identities accessing enterprise resources has only gotten more complicated during the past several years. Between the increasing number of identities, the challenges posed by phishing attacks, and the continued growth of cloud adoption, enterprises are under pressure to ensure the army of remote workers, contractors, and employees accessing network resources are doing so securely and successfully.

Many identity stakeholders have responded by prioritizing identity in the past year. For forward-thinking enterprises, identity is not simply the subject of discussions within the human resources department or the help desk team. It is a critical consideration in security planning as well. With identity-related breaches remaining a continual threat, the business impact of handling identity correctly—and incorrectly—has never been more clear.

In this report from the Identity Defined Security Alliance (IDSA), we revealed just how far along today's organizations are on the journey toward identity-centric security and how far they have to go. Based on data gathered by Dimensional Research, the report captures the realities of more than 500 individuals responsible for IT security or identity and access management (IAM) at companies with more than 1,000 employees.

# The key findings include:

## Identity growth continues, making identity a top security priority




Have identified identities as among the Top 3 priorities for their security program


Said identity investments are part of strategic initiatives


Said the number of identities is increasing, primarily driven by cloud adoption, third-party relationships, and machine identities

## Identity-related attacks rising and impactful, but preventable

**84%** Of respondents said they experienced an identity-related breach in the past year

**96%** Reported that they could have prevented or minimized the breach by implementing identity-focused security outcomes

**78%** Cited experiencing direct business impacts such as recovery costs and reputational damage resulting from such a breach

## Risky behavior reduced when executives put focus on identity security

**72%** Have executives who speak publicly to employees about password security

**60%** 60% of IT/Security stakeholders admitted to risky security behaviors

IT/security stakeholders are more careful with their work passwords when executives speak publicly about their importance

## Investments in security outcomes still a work in progress, focus on basics lacking


Will be investing in identity-focused security outcomes, the same as last year


Typically remove access for a former employee within a day, but only 26% always do

**MFA**

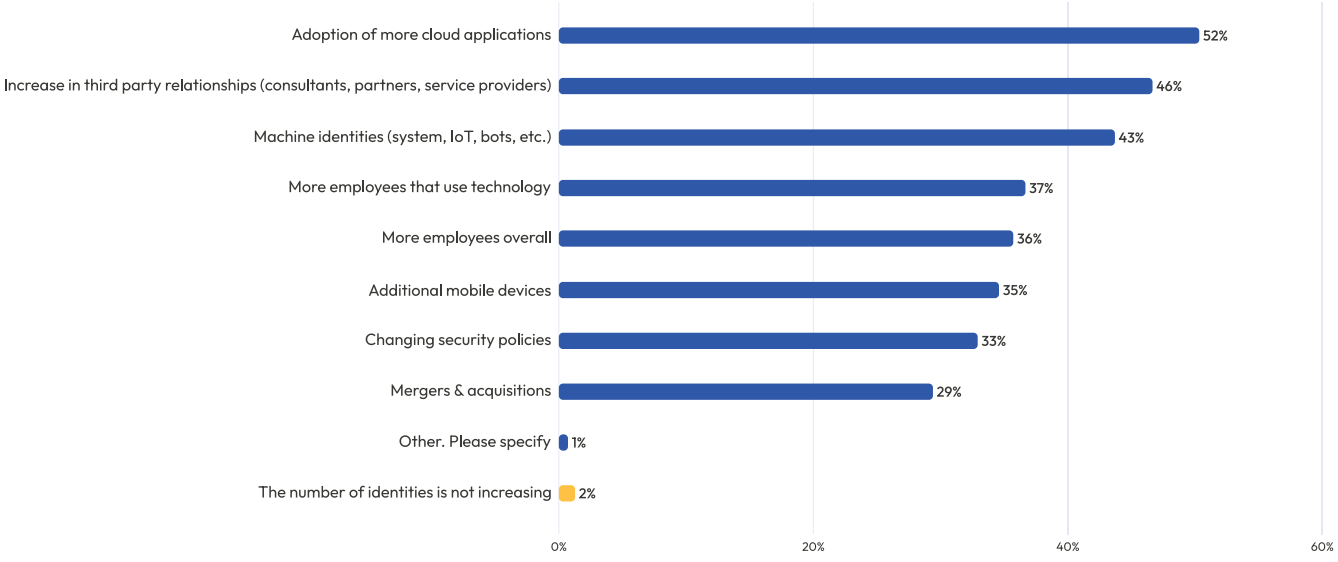
Is a key focus area, particularly for privileged users and employees

# The Current State of Identities and Security

DETAILED FINDINGS:
**Identity growth continues, making identity a top security priority**

Almost all of the identity and security professionals (98%) say that the number of identities in their organization is increasing. The surge in the amount of machine and human identities that organizations now have to manage and secure has several drivers. Overall, respondents cited the adoption of more cloud applications (52%), an increase in third-party relationships (46%), and a spike in machine identities such as bots and Internet-of-Things devices (43%) as the biggest reasons for the increase.

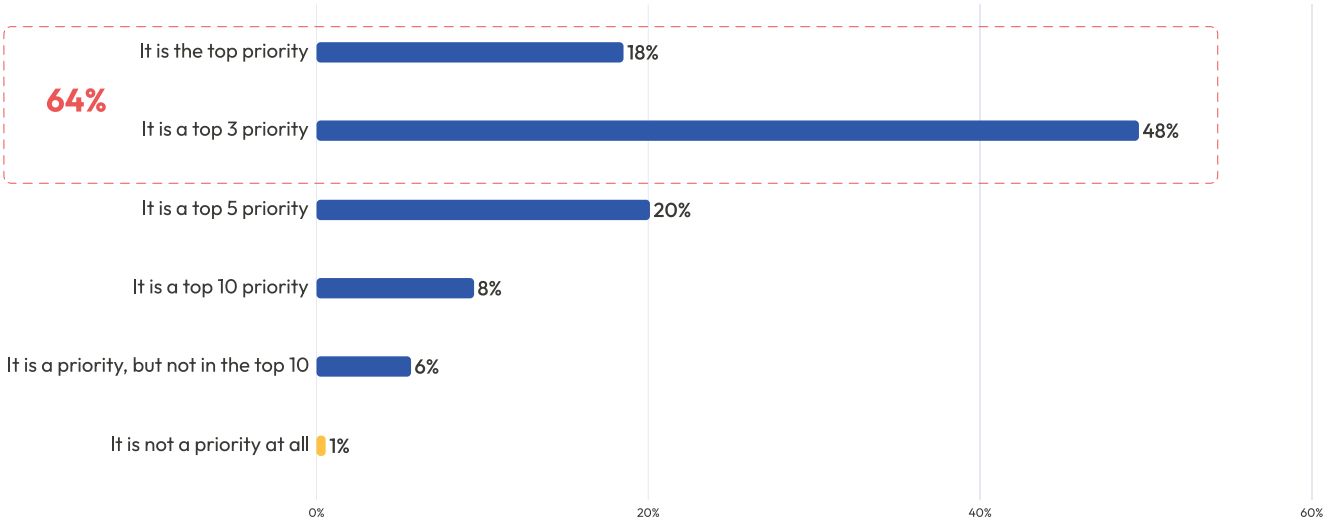
**What is driving an increase in the number of identities at your organization?** Choose all that apply.




Most frequent other response: remote work

This new landscape opens the door to new challenges and risks. In the face of phishing and other identity-related attacks and a world where the traditional network perimeter has been eroded, identity has emerged as the focal point for the security strategy of many enterprises. When asked how much of a priority managing and securing identity is to their security program, a total of 64% of respondents said it is in the top three.

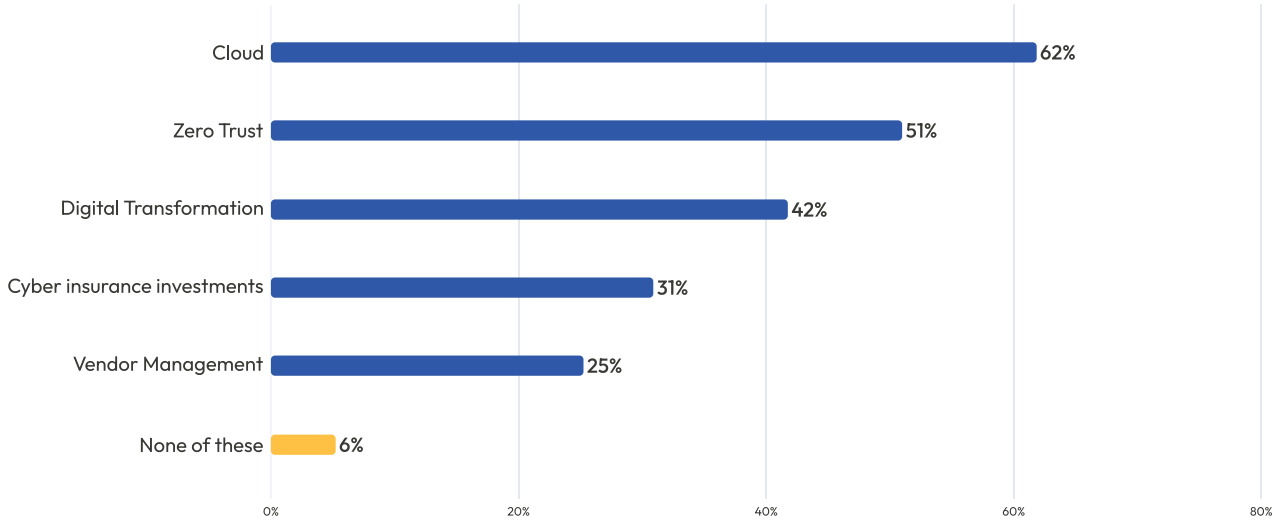
**How would you characterize the importance of effectively managing and securing digital identities within your company's security program?** Choose the one answer that most closely applies.




As the number of identities and the complexity of managing them increases, IT leaders are aligning IAM investments with both security and business goals. Done effectively, IAM creates a secure process for authorization, policy enforcement, provisioning, and deprovisioning that minimizes friction and powers business operations. As a result, IAM is a potential source of improvements in terms of both security and productivity.

The topic of identity is making its way into discussions about the technology plans of enterprises. Overall, 94% of identity and security professionals said their identity program had been included as an area of investment as part of other strategic initiatives in the past year related to cloud, Zero Trust, vendor management, digital transformation, and cyber insurance. Sixty-two percent said identity had been invested in as a part of their cloud adoption strategy, while 51% and 42% said it was included in their Zero Trust implementation and digital transformation initiatives, respectively. Thirty-one percent said it was a part of their cyber insurance investments, an area of growing importance in cyber security strategies and 25% are including identity as part of vendor management efforts.

**In the past year, has your identity program been included as an area of investment as part of any of these strategic initiatives?** Choose all that apply.



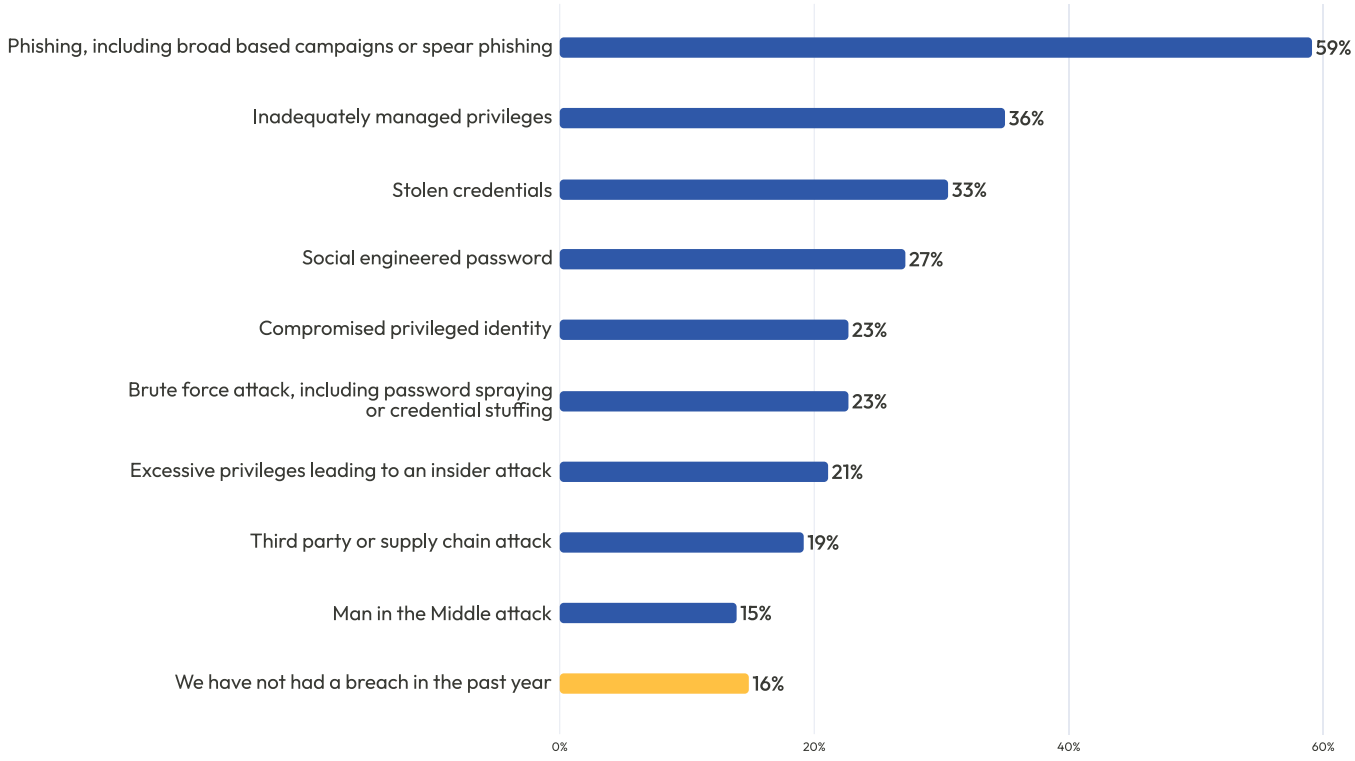

These track with the answers that were given about what participants see as driving the increase in identities. Whether to better control who is accessing cloud resources or implement Zero Trust to enforce the principle of least privilege for a growing army of vendors, many organizations see identity as a piece of the puzzle too important to be ignored.

# The State of Breaches in 2022

**DETAILED FINDINGS:**
**Identity-related attacks rising and impactful, but preventable**

It is an unfortunate but sobering fact that security teams are facing a constant struggle to keep their organizations secure. An alarming 84% said their organization had experienced an identity-related breach in the past year. When asked what kind of breach, the most common answer was phishing attacks (59%), whether broad-based attacks or spear phishing. Other commonly cited causes were inadequately managed privileges (36%) and stolen credentials (33%).

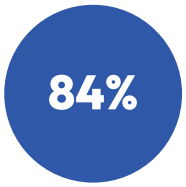
**What kind of identity-related breaches has your company had IN THE PAST YEAR?** Choose all that apply.



Research conducted last year by the Identity Defined Security Alliance, **2021 Trends in Securing Digital Identities**, showed that 79% had experienced an identity-related breach in the past two years. The time frame of the two questions was different (two years in 2021 compared to one year in 2022), which makes it challenging to directly compare the results, but the data distinctly points to an overall increase in the number of identity-related breaches. Just like now, the breaches often involved phishing and the use of compromised credentials. With those credentials in tow, a threat actor can use their access to pivot around the IT environment, steal data, deploy ransomware or take other malicious actions.

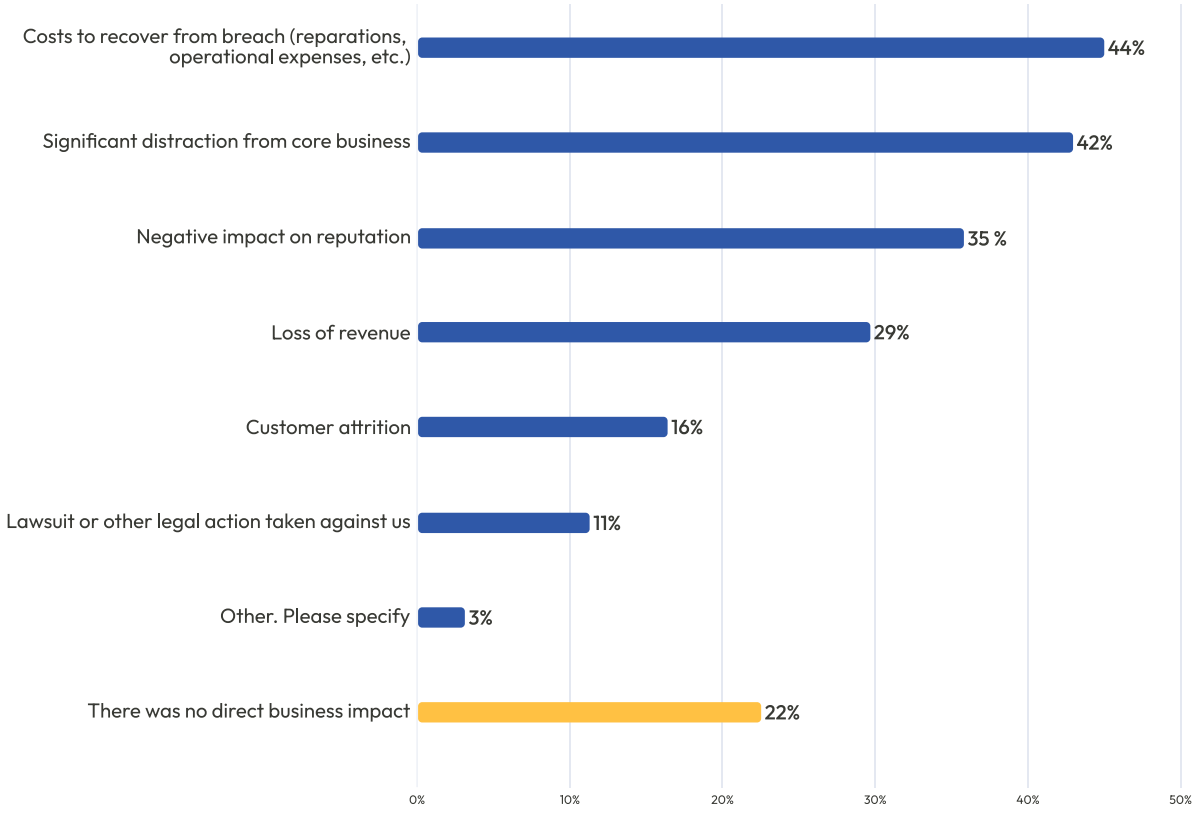
**Company has had an identity-related breach in the past two years.**


**Company has had an identity-related breach in the past year.**



The metaphorical—and actual—price tag for these breaches can be high. According to our 2022 study, 78% of those who experienced an identity-related breach said it was associated with a direct business impact. Forty-four percent noted the cost of recovery, and 42% said it caused a significant distraction from the organization's core business. Thirty-five percent noted a negative impact on the organization's reputation. Customer attrition (16%) and loss of revenue (29%) were also cited. Other business impact responses included, purchase additional equipment, loss of confidence from stakeholders and required additional training.

**Did your organization suffer any direct impact to business results as a result of identity-related breaches in the past year?** Choose all that apply.

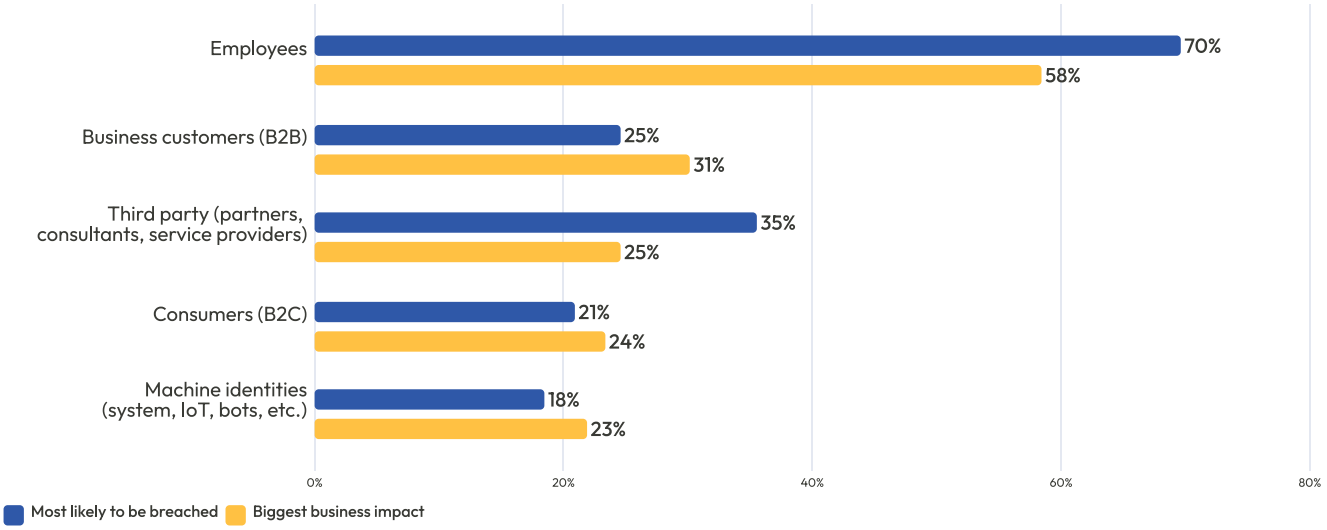


When asked about impacts to the organization more generally, common responses included: malicious attacks on applications or systems (32%), a period where IT systems were unavailable or degraded (28%), and products, services, or solutions delivered by the organization being compromised (21%). Interestingly, some responded to the question about more general impacts by stating that they did not know (13%) or that there was no impact (14%). There could be a variety of reasons for this feedback, including stealthy tactics by attackers.

Employee identities were viewed as the most likely to be breached (70%), with third-party vendors and B2B customers coming in second and third, with 35% and 25%, respectively. Fifty-eight percent believe that employee identity breaches would result in the biggest direct business impact. This finding may be due to the potentially higher access levels they have compared to non-employees.

**In your opinion, what type of identity is most likely to be breached?** Choose up to 2 of the following.

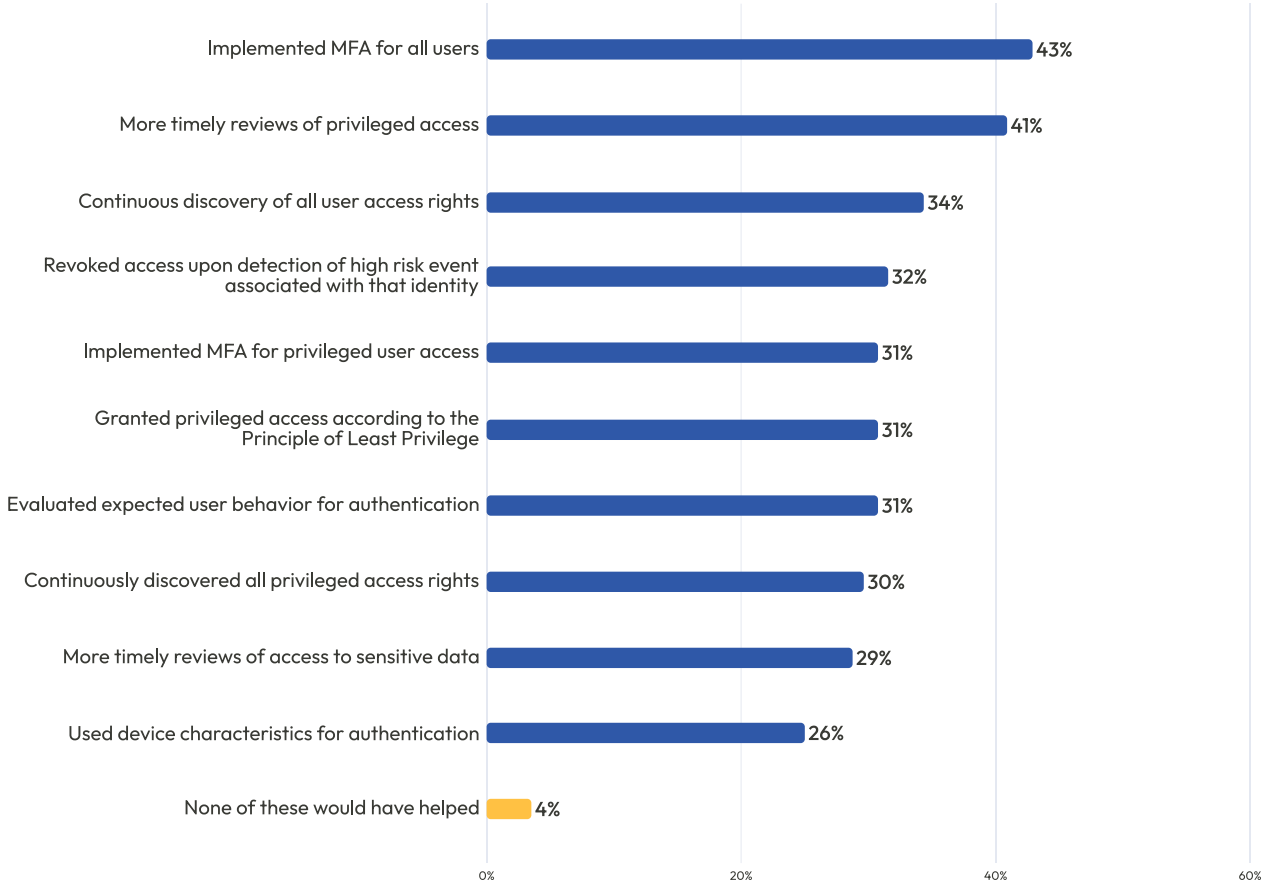
**In your opinion, what type of identity breach would result in the biggest direct business impact?** Choose up to 2 of the following.



These numbers supplement other IDSA research from recent years that shows identity-related breaches remain commonplace. The key to successfully addressing them is to raise the barrier to entry for attackers, and **IDSA's security outcomes** do exactly that. IDSA defines security outcomes as capabilities that help organizations establish an identity-centric approach to security that reduces the risk posed by data breaches.

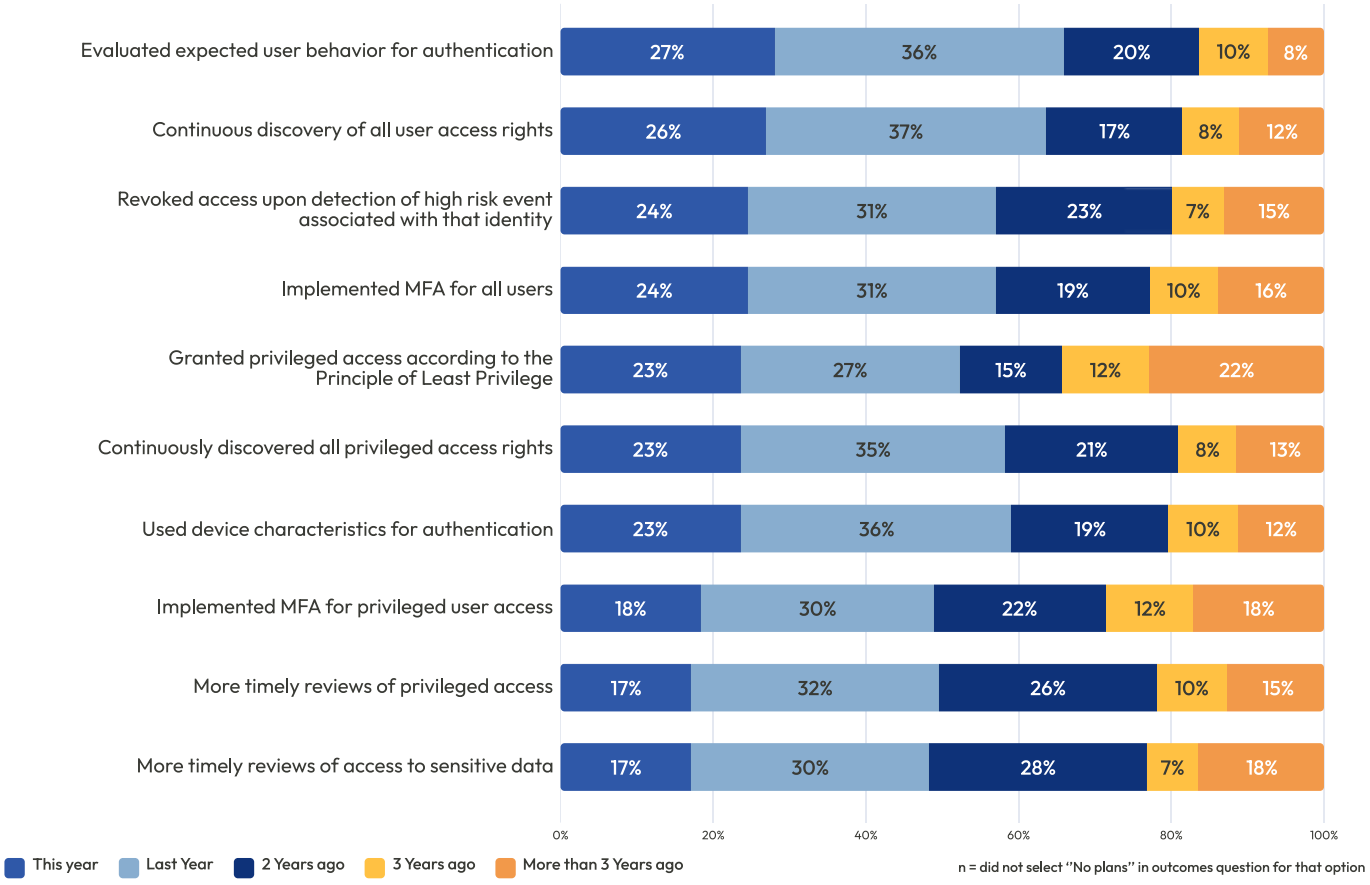
Centered on enabling effective identity governance, access, and behavioral detection, the security outcomes add a layer of protection around IT environments. Those surveyed almost universally agreed—96% reported that, in retrospect, implementing a security outcome could have prevented or minimized a breach. It is here that multifactor authentication as a mitigation strategy jumped to the top of the list in preventing breaches. Forty-three percent believed that implementing MFA for all users would have made a difference. The next most common responses were more timely reviews of privileged access (41%) and continuous discovery of all user access rights (34%).

**In retrospect, could any of the following have prevented or minimized the breach?** Choose all that apply.



The good news: the prevalence of data breaches has driven organizations to make progress on implementing IDSA's security outcomes, with many respondents stating their organization had begun the process of planning or adding these capabilities in the past year.

**When did your company first begin planning or implementing each of the following?**

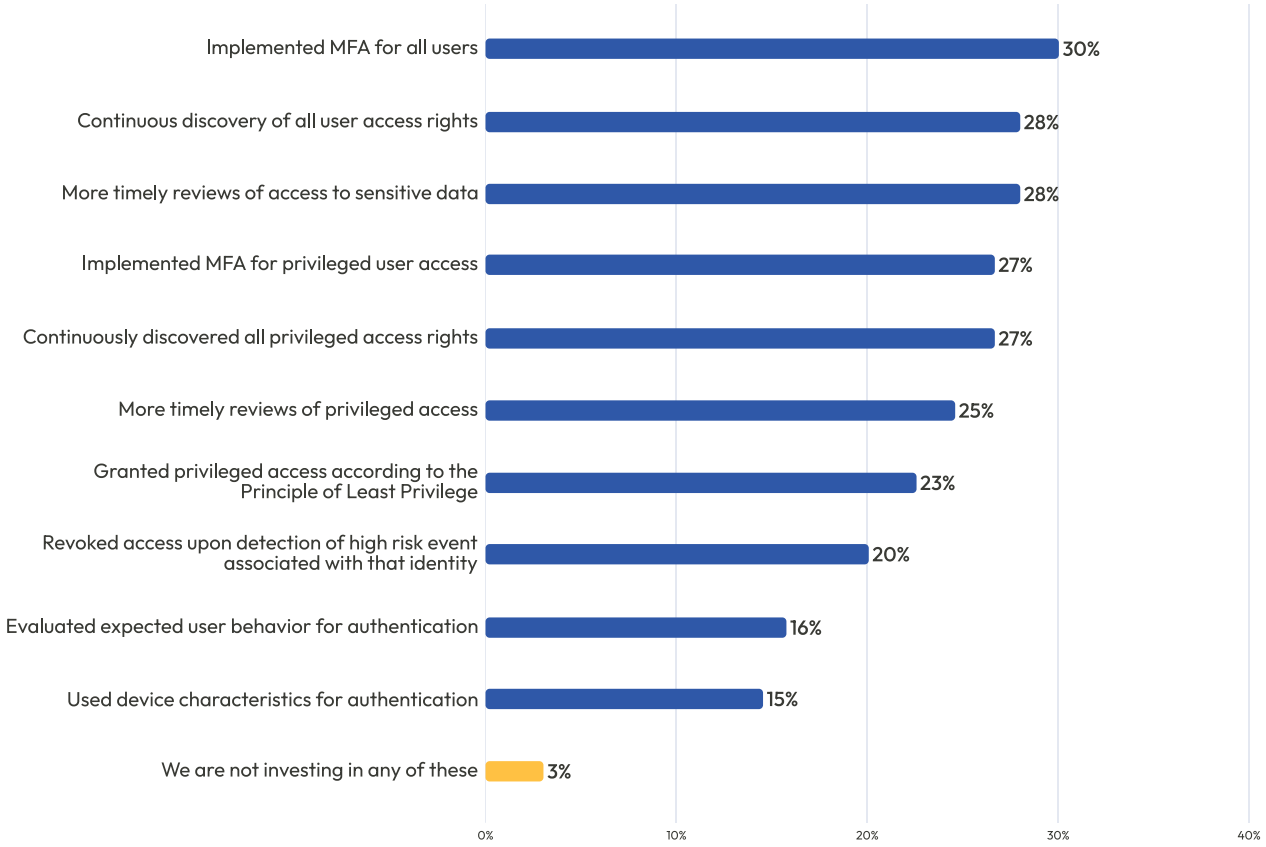


# The State of Prevention in 2022: Technology and Expertise Trends

**DETAILED FINDINGS:**
**Investments in security outcomes still a work in progress, focus on basics lacking**

The old saying that an ounce of prevention is worth a pound of cure still rings true in IT security. Virtually all of the security and identity pros—97%—said their organizations would invest in identity-focused security outcomes in the next year. Enforcing MFA for all users, reviewing sensitive data access, and continuously discovering user rights are the three biggest investment areas for the coming year. Among those who said that implementing MFA for all users would have minimized the impact of breaches they suffered, 38% specifically cited fully implementing MFA for employees as a capability that would have reduced the negative impact. MFA for third parties was next on the list, cited by 17%.

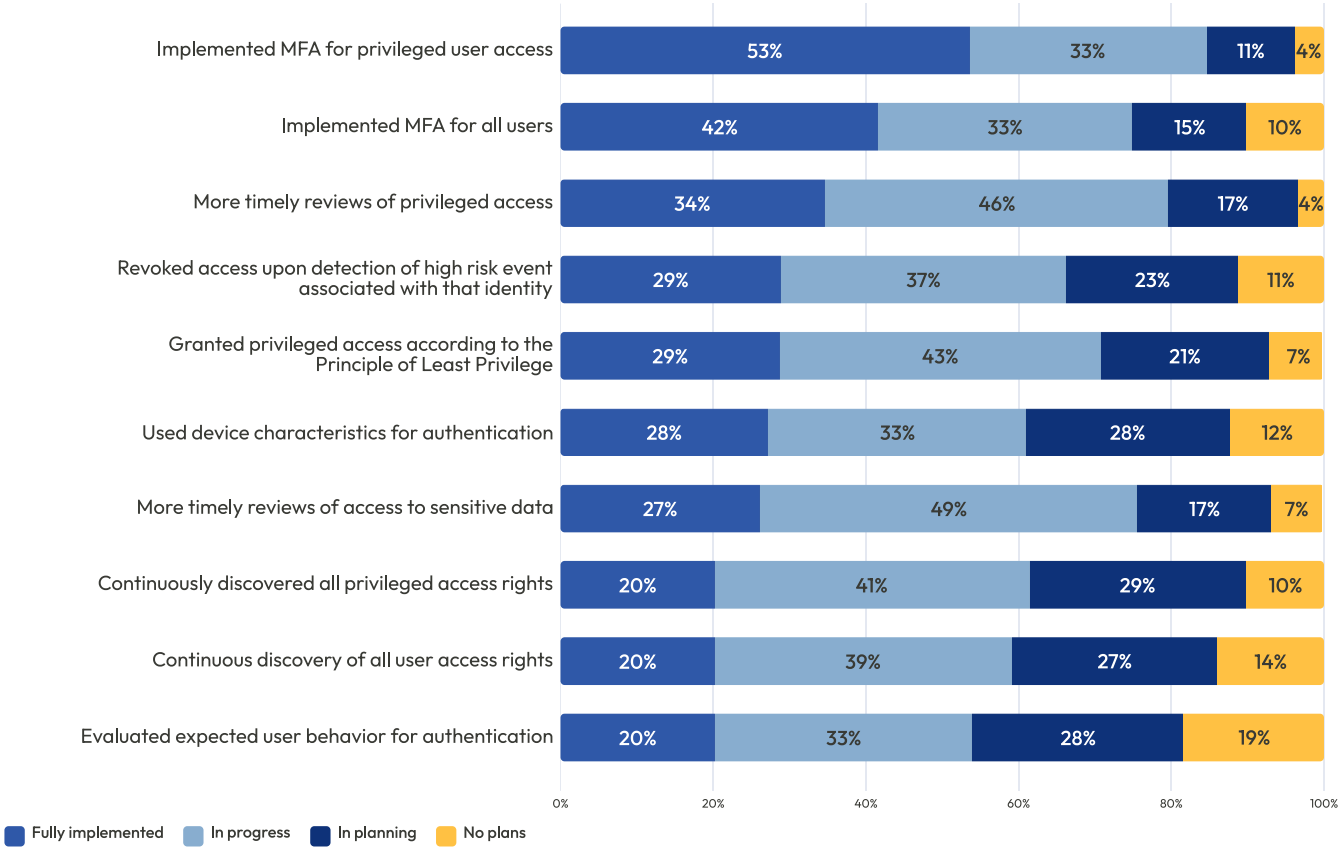
**Which of the following is your company investing the most in over the coming year?** Choose up to three of the following.




Most frequent: Conducted additional training

For many organizations, the implementation of security outcomes was largely a work in progress. For example, 46% of organizations overall described the implementation of more timely reviews of privileged access as “in progress.” Thirty-nine percent said enabling the continuous discovery of all user access rights is “in progress,” while 20% said it was fully implemented. Even the enforcement of the principle of least privilege is lacking, with 29% describing the ability to grant privileged access based on least privilege as “fully implemented” and 43% stating implementation efforts are still “in progress.”

**Below is a list of possible identity-related security outcomes. What is your company current level of implementation for each of these?**

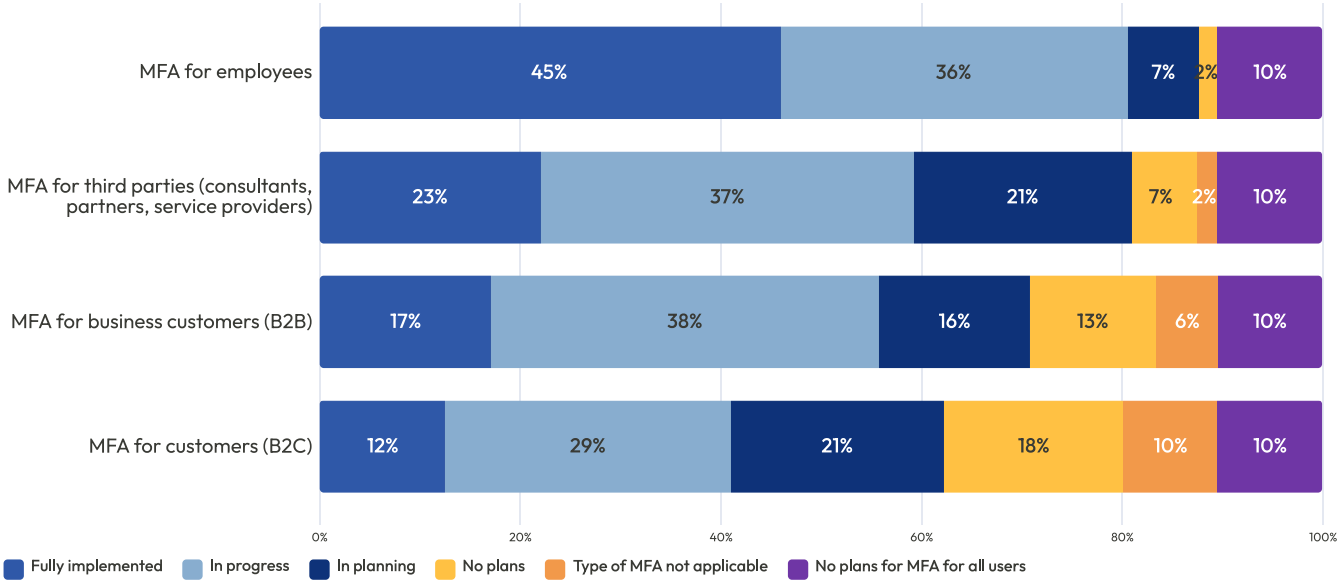



As always, security is still about defense in depth—leveraging multiple security controls and measures to create layers of security that protect your environment. Integrating identity and security functions and implementing capabilities like MFA, user behavioral analysis, and the assessment of device characteristics takes organizations closer to a Zero Trust environment and reduces the risk of data breaches.

A staple of many of today's data breaches is credential theft. In response, enterprises frequently turn to MFA mechanisms such as biometrics and SMS messages as a solution. Requiring another means of authentication—particularly for privileged users—reduces the risk posed by attackers abusing legitimate credentials, who will also have to be in control of a second, out-of-band form of verification to gain access.

With breaches of employee identities being the most feared, it should come as little surprise that MFA for employees is the most likely to be fully implemented. Being employees, they may have greater privileges than the typical contractor and, unlike contractors, are likely to maintain their access rights for longer as they are not temporary workers. As a result, employee identities represent a juicy target for attackers. Still, MFA for third parties such as consultants and service providers was the second most likely to be fully implemented, and efforts to implement MFA for business customers, third-party vendors, and employees were the most frequently reported as being "in progress."

**Below is a list of possible identity-related security outcomes. What is your company current level of implementation for each of these?**




n = all (asked only to those that have started MFA for all users, but graph calculated to show all)

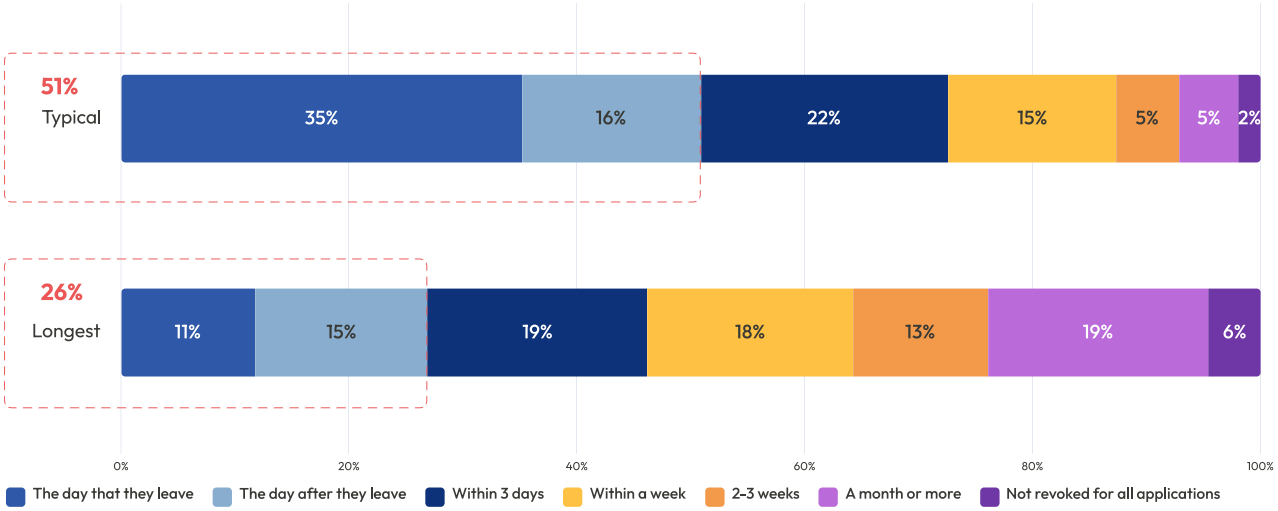
Regardless of the type of user, poor identity governance processes for deprovisioning identities can create orphaned accounts. These accounts, which no longer have valid owners, present opportunities for attackers to abuse the trust and privileges given to previously legitimate users. For this reason, they leave organizations particularly vulnerable to disgruntled former employees who may want to steal data or take other malicious actions. Other threat actors can take advantage as well, as these accounts may be out of compliance with security policies and lack an owner who may notice their account is being misused.

Only 51% of organizations in our survey said they typically remove a user's accessto corporate systems the day (35%) or the day after (16%) the employee leaves. These percentages are comparable to the findings in our **Identity and Access Management: The Stakeholder Perspective report**, which revealed that 34% of line-of-business identity stakeholders said that access is revoked the day an employee leaves and 15% said the day after.

The fallout from failing to remove access can be severe. In the case of the notorious Colonial Pipeline attack in 2021, a legacy VPN profile no longer in use by the company was compromised to launch the attack. The account was not protected by MFA. The incident led to a spike in gas prices in the US, and it took the company more than a week to resume normal operations.

**In your experience, how long does it TYPICALLY take to remove access to all corporate systems for an employee who leaves?** Choose the one answer that most closely applies.

**In your experience, what is the LONGEST time it has taken to revoke access to all corporate systems for an employee who leaves?** Choose the one answer that most closely applies.



# The State of Prevention in 2022: Culture and Human Behaviors

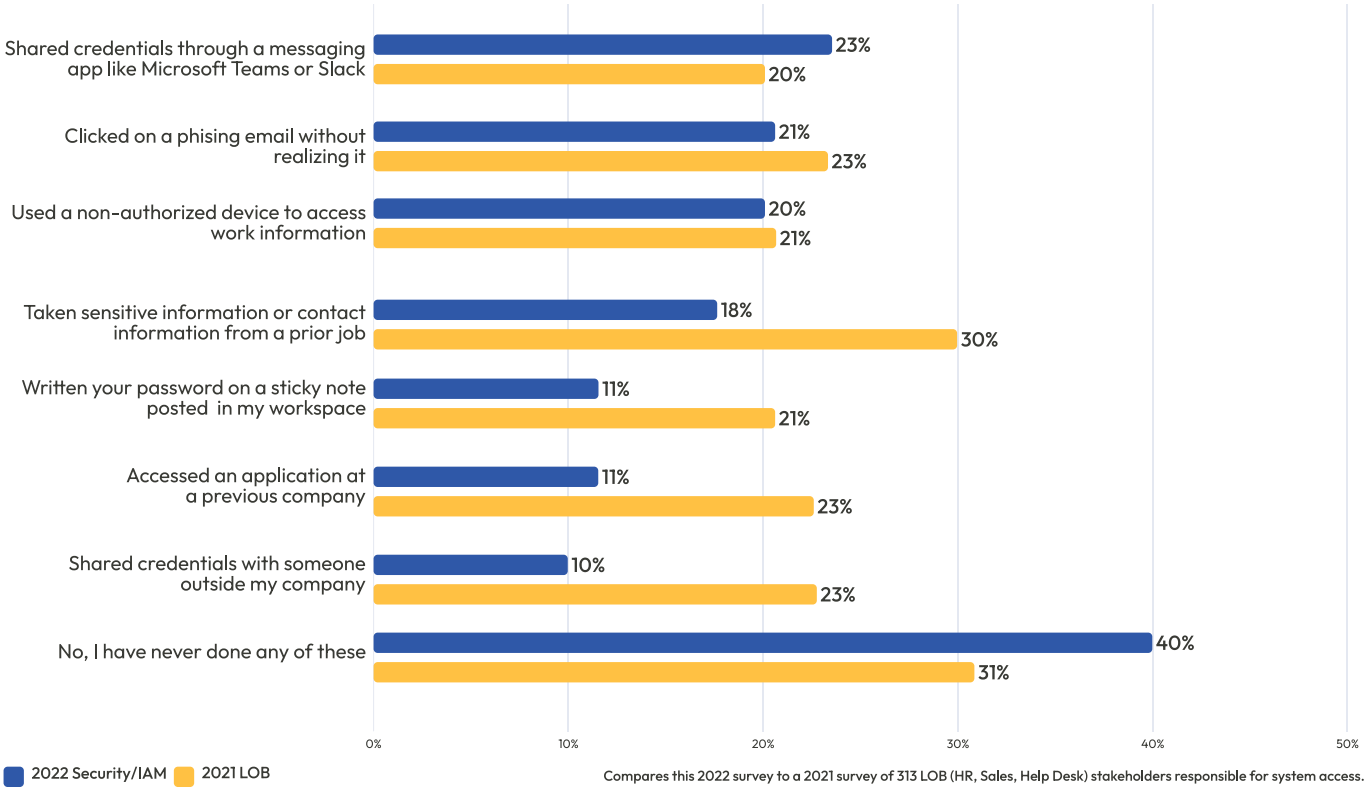
DETAILED FINDINGS:

**Risky behavior reduced when executives put focus on identity security**

Not all solutions to security challenges are technical. Sometimes, the biggest challenges to security are people. Technical controls can be undone by weak passwords, password sharing or other actions taken by careless employees and trusted third parties like vendors and contractors.

Even security users are often guilty of not following best practices. Sixty percent of security professionals admitted to engaging in risky behaviors, compared to 69% of line-of-business users surveyed in The Stakeholder's Perspective study conducted last year. While 40% of security pros said they did not engage in the risky behaviors we asked about, 23% admitted sharing credentials through a messaging app like Microsoft Teams or Slack. Twenty percent said they used a non-authorized device to access work information.

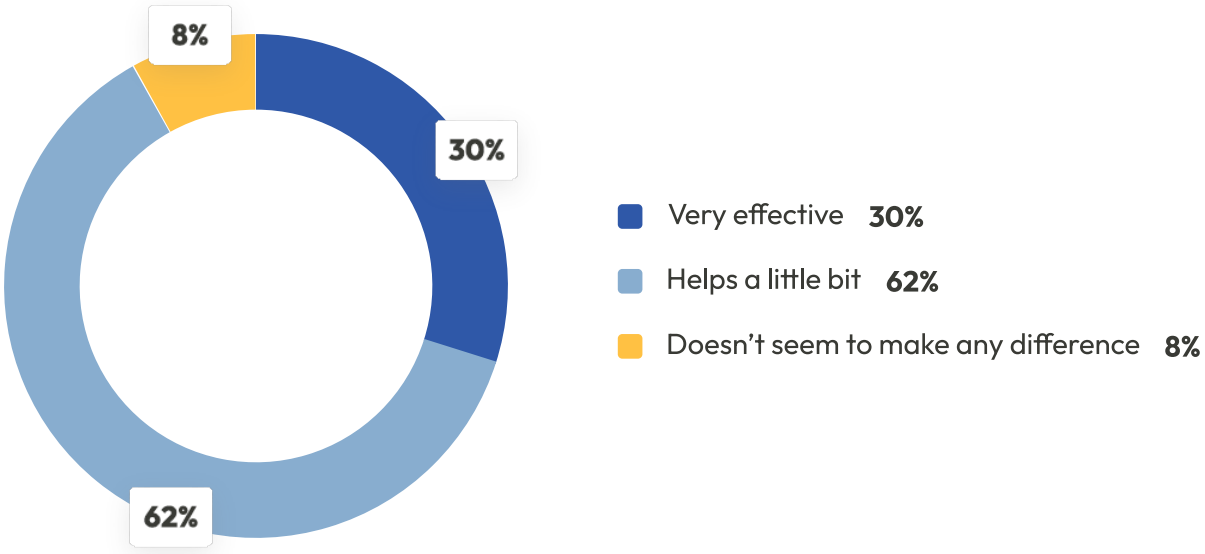
**Have you personally done any of the following?** Choose all that apply.




Compares this 2022 survey to a 2021 survey of 313 LOB (HR, Sales, Help Desk) stakeholders responsible for system access.

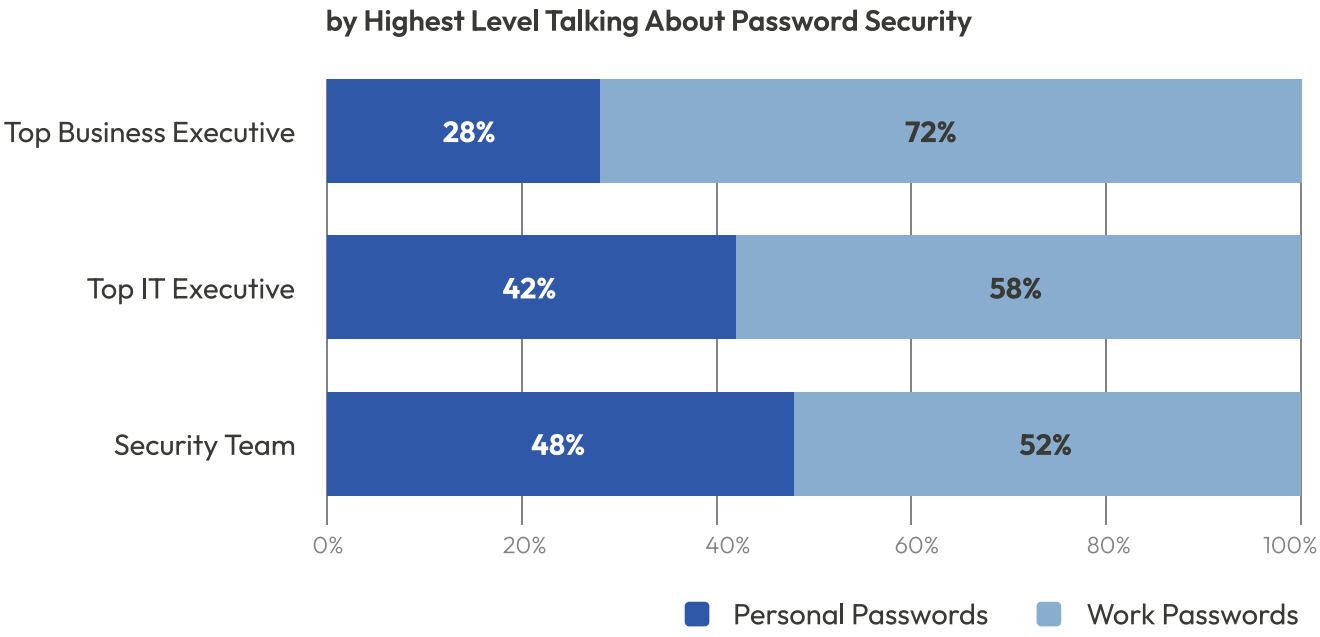
While training on password security is ubiquitous (94%), only 30% described the training as “very effective”, while 62% said it helped “a little bit.” Eight percent said it didn’t seem to make any difference.

**In your opinion, how effective is the training on securing passwords that your company provides employees?** Choose the one answer that most closely applies.




Sixty-five percent said their organization provides mandatory training on password security on a regular basis (e.g. quarterly, yearly). For many certifications like SOC 2 and ISO, this is a requirement but is proving to empirically be ineffective. What did have an impact is executive support. More than than 70% of organizations have executives speaking about the topic. When asked who the highest level executive who talks to them about password security is, 51% said the "CIO, CISO, or other top IT or security executive." Even identity and security stakeholders do better when leadership is engaged—72% said they were more careful with their work passwords than their personal ones had a top-level business executive speaking about password security.

**Are you personally more careful with your personal passwords or your work passwords?**



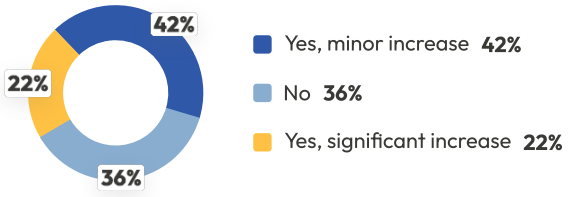
# Special report: The Impact of Russia/ Ukraine crisis

## The conflict in Ukraine is bringing more visibility to security.

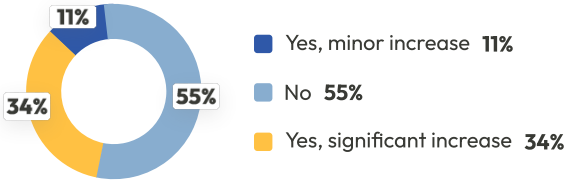
Sometimes news events impact the attention being paid to cyber security by executives. In 2020, it was the COVID-19 pandemic, a situation that led to an increased focus on cloud security and the additional risks tied to supporting a mobile workforce. This year, we must consider the crisis in Ukraine. Even before the invasion in February, cyberattacks in Ukraine led to concerns in the U.S. that the Russian government could launch cyber-operations that would disrupt not only organizations in Ukraine but also critical infrastructure in the U.S. In May, the U.S. accused Russia of conducting cyberattacks against targets in Ukraine during the buildup to the fighting as well as afterward. The conflict brought cyber security directly into focus for business leaders worried about the impact it could have on their operations.

Sixty-four percent of respondents said the situation in Ukraine has increased the amount of attention non-technology executives were paying to identity management and security activities. However, budget increases have not been in step with the spike in attention, with just 45% overall seeing either a minor or significant increase. The largest budget increases were among financial and healthcare companies. Some 35% of respondents from the financial industry reported a significant bump, while another 30% stated they saw a minor increase. For healthcare organizations, the numbers were 25% and 46%, respectively.

**Has the recent Russia/Ukraine crisis increased visibility of your company's identity and security activities among non-technology leadership?**



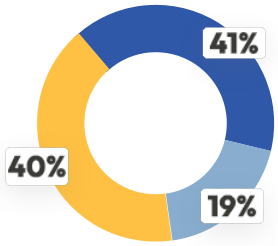

**Has your company increased budgets for identity and security activities as a result of the Ukraine/Russia crisis?**



## Survey Methodology and Participant Demographics

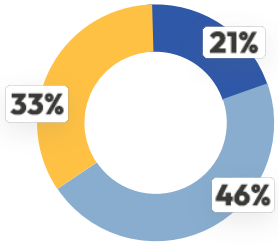
An online survey was sent to independent sources of security and identity professionals in the United States. A total of 504 qualified individuals completed the survey. All participants were directly responsible for IT security or IAM at a company with more than 1,000 employees. Each was very knowledgeable about both IT security and identities. Participants included a mix of company sizes, job levels, and industries.

### Company Size



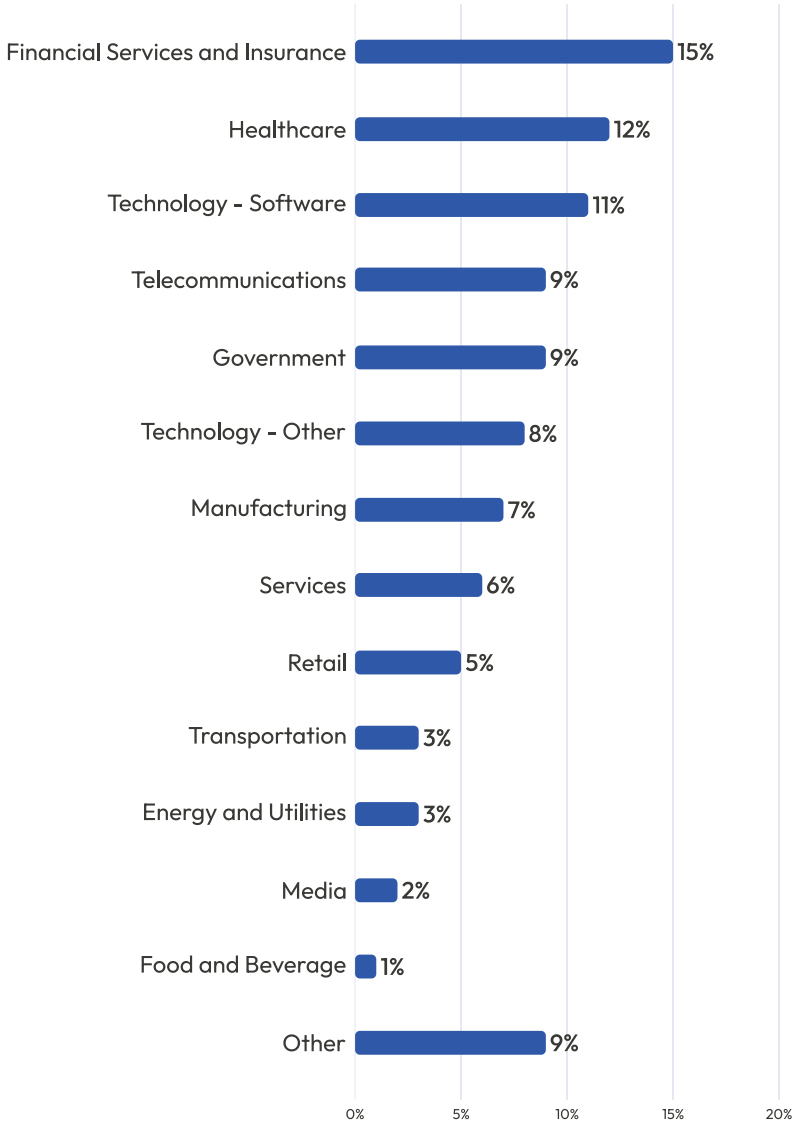

- 1,000-5,000 employees **41%**
- 5,000-10,000 employees **19%**
- More than 10,000 employees **40%**

### Job Level




- Executive **21%**
- Team Manager **46%**
- Individual Contributor **33%**

### Industry



## 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**.