RSA

RSA.com

2025 RSA ID IQ Report

A global survey of identity and access management, AI, passwordless, and the cost of data breaches

Table of Contents.

Executive Summary.

In 2023, RSA ran the ID IQ Quiz, which asked participants difficult questions about the definition of Zero Trust, the frequency of password reuse, and what capabilities defend against identity-related attacks.

We were surprised—if not a little shocked—at some of the answers we got back. Nearly half of all users got at least half the questions wrong, with self-described identity and access management (IAM) and cybersecurity experts performing the worst. We also found optimism about AI's cybersecurity potential and significant vulnerabilities in unmanaged devices used as professional resources.

We wanted to learn more, including how much low identity security knowledge cost organizations, whether organizations were putting their money where their mouth was on AI, and if there was a chance to close the personal device security gap. Given the noise and potential of passwordless, we also wanted to know whether organizations were really making changes to their authentication strategies.

What we learned

The 2024 RSA ID IQ Report reveals how frequently identity-related breaches affect organizations, the impact those breaches make on an organization's bottom line, and the investments that organizations are making in their identity capabilities:

- **When organizations suffer identity-related data breaches, it costs them—significantly:** Identity-related data breaches are more severe and costly than run-of-the-mill incidents: More than 40% of respondents reported an identity-related security breach. Of those, 66% reported it as a severe event that affected their organization. 44% of respondents estimated that the total costs of identity-related data breaches exceeded the cost of a typical data breach. These findings underscore why organizations should prioritize investing in security capabilities that can mitigate the high costs of identity-related breaches.

- **Cybersecurity is no longer on the fence about AI:** 80% of respondents felt that AI will do more to empower cybersecurity than abet cybercriminals over the next five years, with nearly as many organizations (79%) planning to implement some AI in their cybersecurity stack within the next year. Entertainment, finance, and retail were the likeliest sectors to implement some form of AI in the next year. Highly regulated industries are among the most likely to have plans to implement AI in their cybersecurity stacks.

- **Organizations are leaving toxic relationships with passwords:** More than half (51%) of respondents reported needing to input their passwords six times or more for work every day. That friction and the cost of identity data breaches may be motivating organizations to change their authentication strategies: 61% of respondents expressed that their organization had plans to implement passwordless capabilities in the next year, rather than wait for phishing or other attacks to breach their defenses.

- **Security software on personal devices divides organizations:** Willingness to install security monitoring software on personal devices varied widely among respondents. 73% of IAM experts and 60% of cybersecurity specialists expressed willingness to have corporate security software on their personal devices, as opposed to only 39% of generalists.

- **Hybrid environments dominate:** 70% of organizations operate in hybrid environments, reflecting the increasingly complex landscape of application and security deployments, and organizations' need for solutions that span environments.

What organizations should do next

I won't keep you from reading through our findings much longer, except to say what I think organizations should take from the research, and what they should do next:

- Whether it's the fear of data breaches, the pain of passwords, or the potential of AI, organizations are prioritizing identity security capabilities. Those that don't stay current risk falling behind—and being breached.
- There is a sharp divide between security specialists and rank-and-file users on implementing security controls on personal devices. Organizations should find a middle ground between the two, because keeping the status quo is untenable.
- The majority of organizations are working in hybrid environments, with some mix of resources spread between hybrid, cloud, and on-premises environments. But if the July 19 CrowdStrike / Microsoft outage was any indicator, most organizations simply don't have the infrastructure needed to manage true hybrid. The outage affected more than 8 million devices and cost the Fortune 500 billions of dollars—if that's not a wake-up call to implement resilient technology, then I don't know what will be.

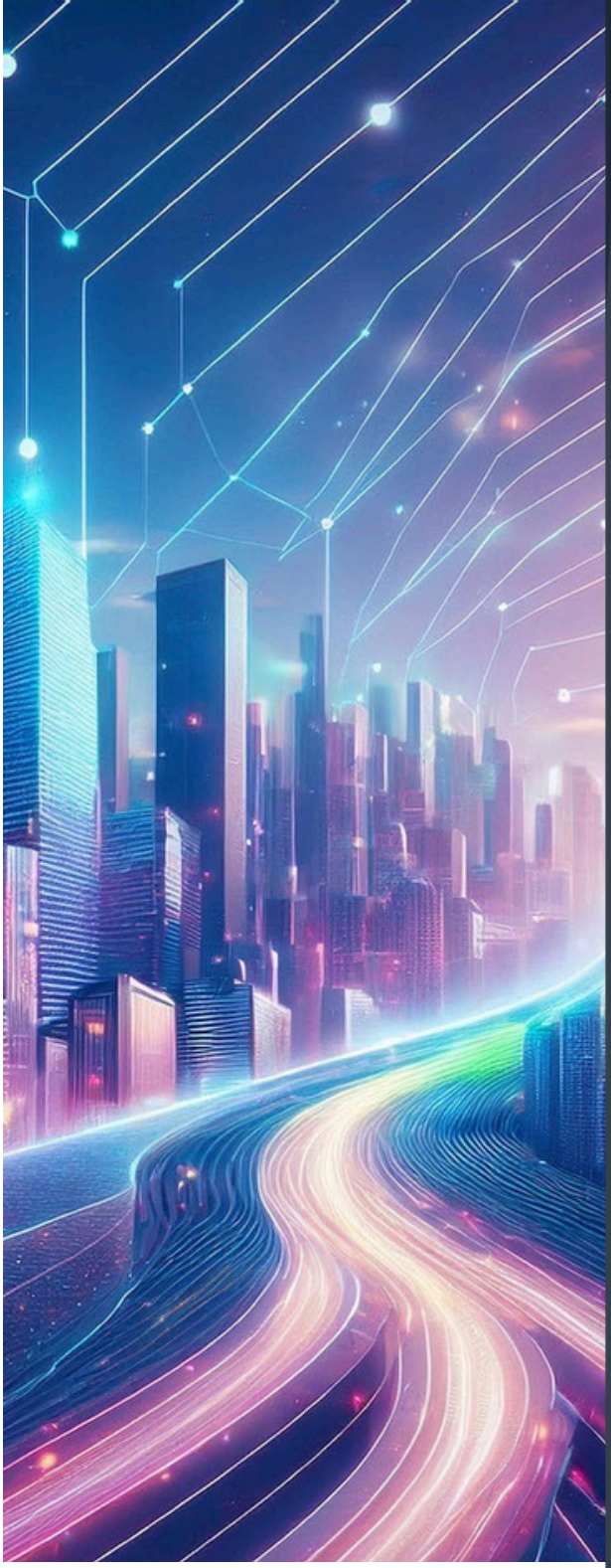
Identity has always been elemental to every part of an organization—it's core to onboarding new users, defending against threats, complying with regulations, and executing operations. That hasn't changed.

What has changed are the forces that act on identity. From AI to cybercriminal activity to new protocols set to disrupt decades of username/password authentication, change is on the way. Our customers seem to be cautiously optimistic about what lies ahead and are committed to the new technologies that will distinguish this new era. They're hopeful about what's to come—but they're not letting their guard down, either.

I think that's precisely what identity must be: willing to embrace the future, but never overlooking its dual roles as an organization's shield and an attacker's target. The future might be bright, but we can't let the glare distract us from the essential work that we do every day.

Rohit Ghai

CEO, RSA

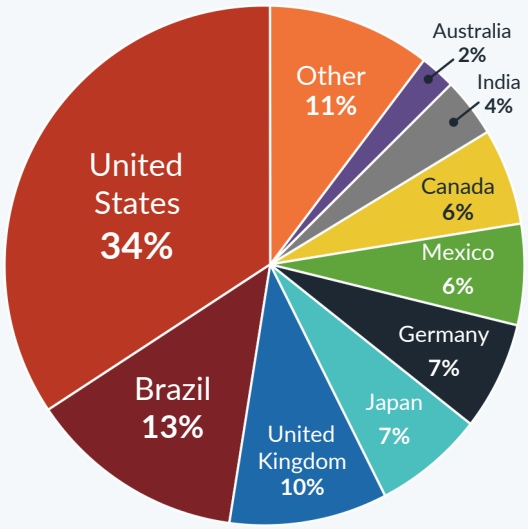


RSA®

Demographics and methodology.

RSA conducted the 2024 RSA The RSA ID IQ Survey took place May 7 to August 1, 2024. In that time, the survey received 2,141 responses from 62 countries. Respondents were asked 20 questions to assess the challenges, opportunities, and working realities that they encountered with multi-factor authentication MFA, passwordless, AI, data breaches, and more.

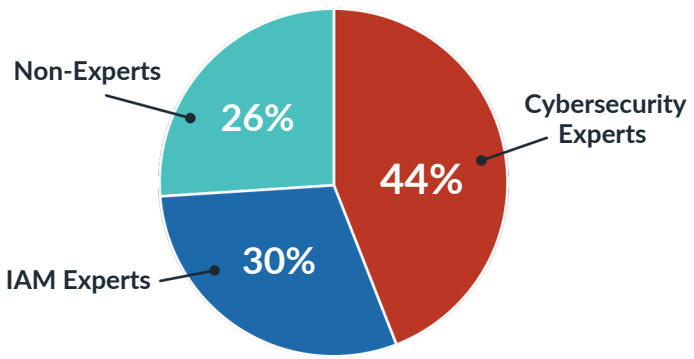
2024 RSA ID IQ Report Respondents, by Country



Expertise

Before answering questions, respondents were asked to identify their role within their organization, categorizing themselves as either an identity and access management (IAM) expert, a cybersecurity expert, or a non-expert.

2024 RSA ID IQ Report Respondents, by Role

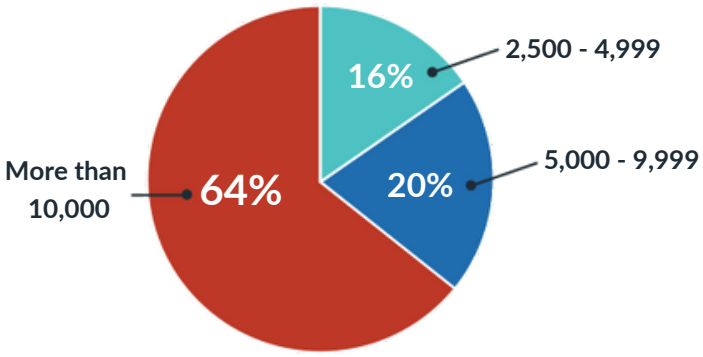


The survey over-indexed on experts, with 44% identifying themselves as cybersecurity experts and 30% identifying themselves as IAM experts. The remaining 26% said they were non-experts.

Industries

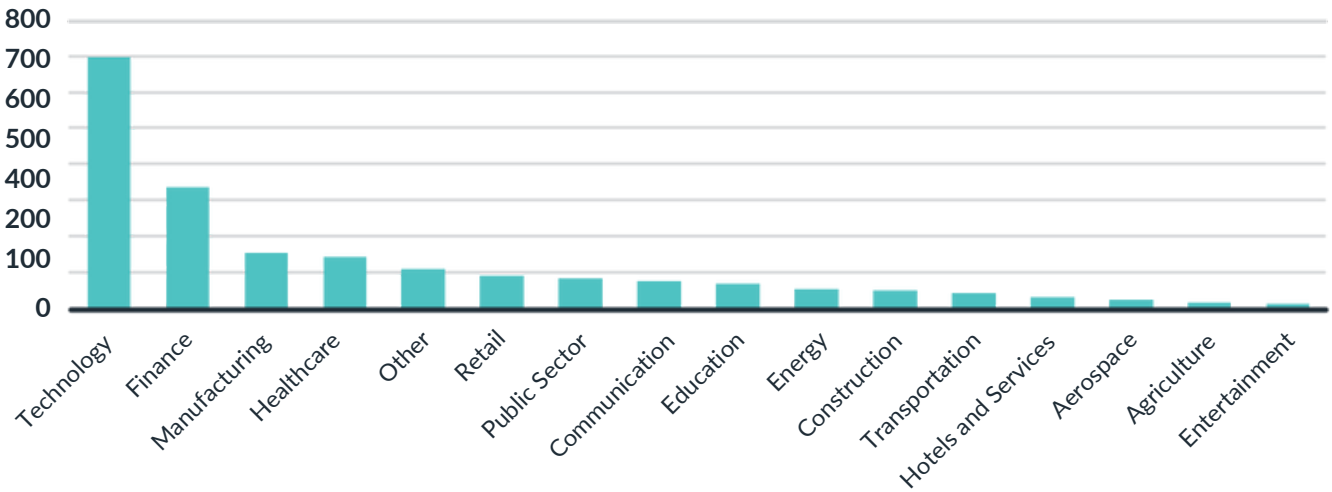
Given that RSA promoted the 2024 RSA ID IQ survey to its customers, the size of respondents' industries and the sectors that they work in largely track with RSA's customer base. The majority of respondents work at large enterprises, with nearly two-thirds (64%) working at companies with more than 10,000 employees.

Respondents' Company Size



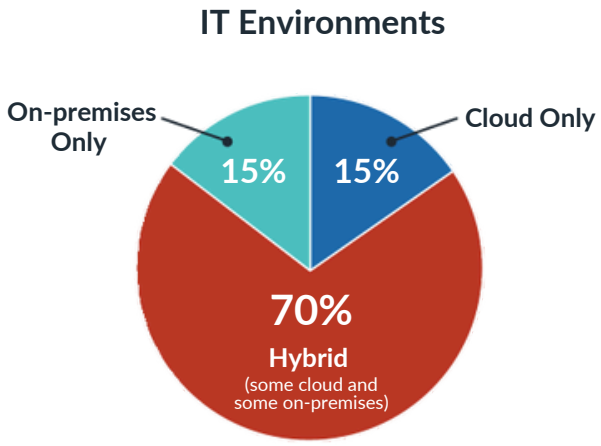
Respondents' sectors also largely tracked with RSA's customer base, with a significant number of respondents working in technology and finance. Manufacturing, healthcare, retail, and public sector agencies also were among the most represented sectors in the 2024 RSA ID IQ Survey.

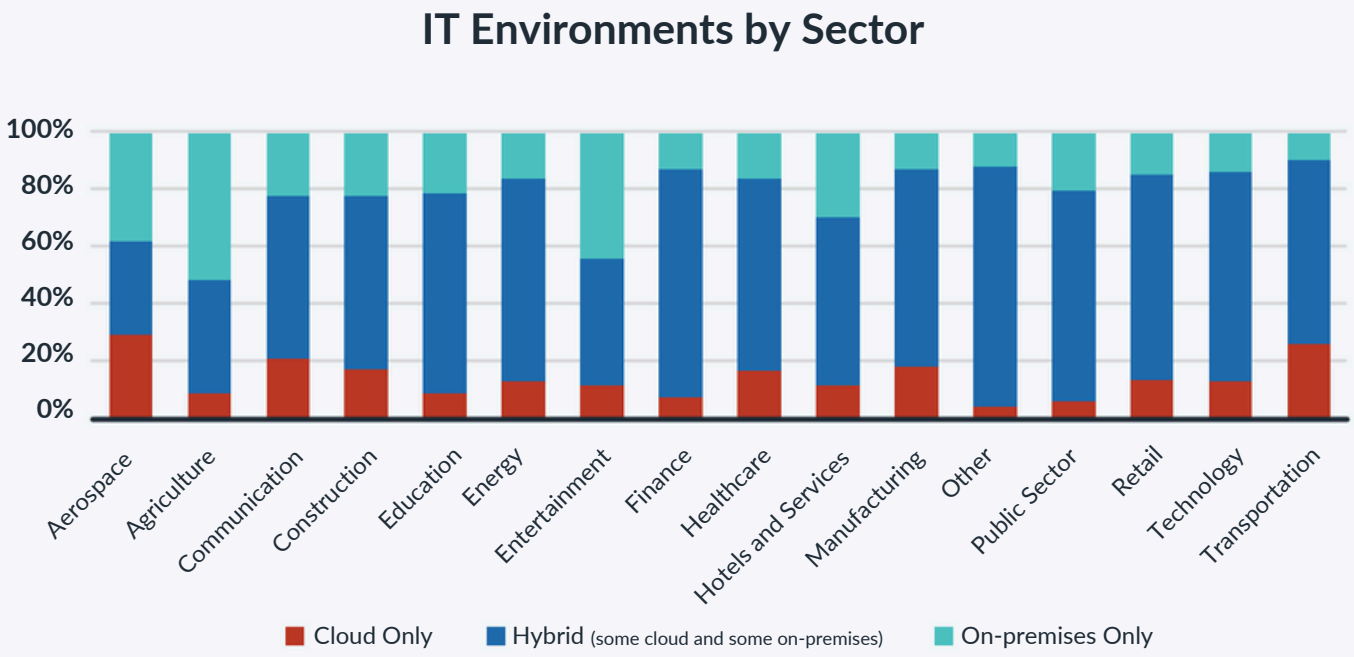
Respondents' Sectors



Environments

The survey asked respondents to identify whether they use on-premises, cloud, or hybrid environments to operate user or security applications. Overwhelmingly, 70% of organizations operated in a hybrid environment, with some use of both on-premises and cloud applications. Only 15% of organizations used only the cloud or only on-premises applications.



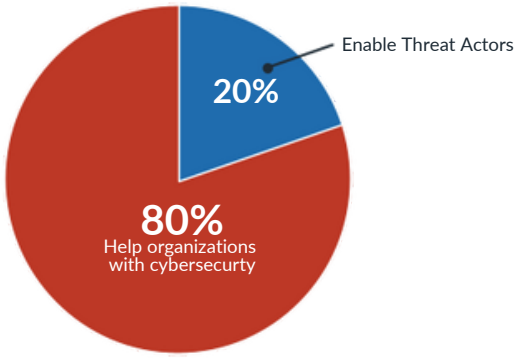


Results and analysis.

Cybersecurity: No longer on the fence about AI.

There are any number of even-handed reports noting that AI is a double-edged sword. Whether it's AI's potential in healthcare, national security, patent law, or climate change, the one thing that experts agree on is that AI has the potential to both do harm and be of real value.

Will AI Help Cybersecurity

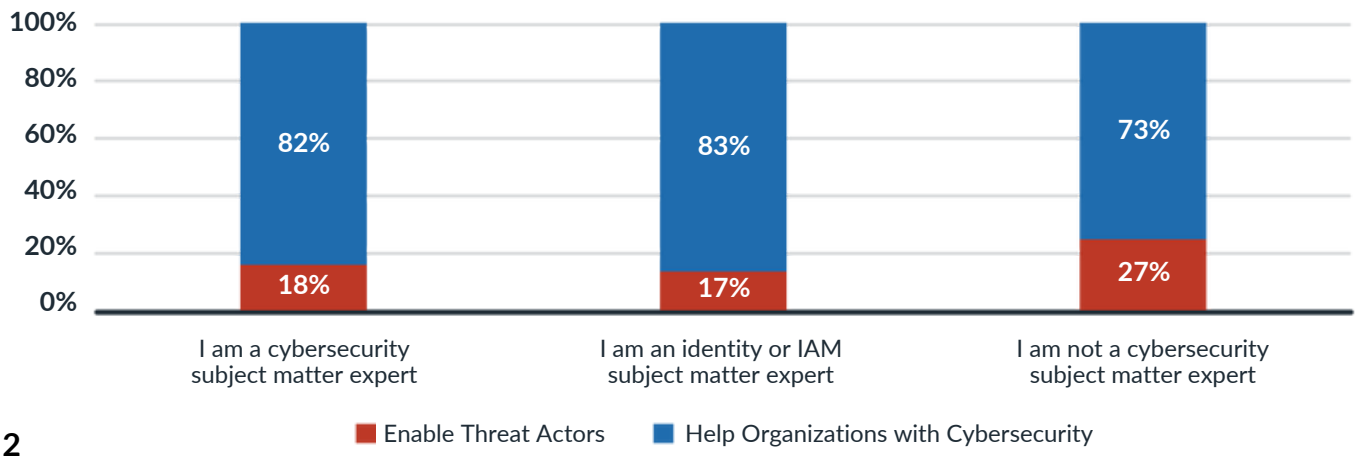


We're guilty of this even-handedness as well. RSA's Top Trends in Identity for 2024 noted that AI was a double-edged sword that would cut even deeper this year and noted that AI had "a lot of potential, both as a new risk and as a new cybersecurity tool."

While we acknowledge that any technology—let alone something as complex as AI—has the potential for dual use, we wanted to see whether users felt it would help cybercrime or cybersecurity more over the next five years.

That's why we asked an either/or question. And the responses were largely positive: 80% of respondents felt that AI will help organizations with cybersecurity over the next five years. Only a fifth felt that AI would do more to enable threat actors in that time.

By Role



Experts were also more inclined to believe that AI would assist cybersecurity more than cybercriminals: 82% of cybersecurity experts and 83% of IAM experts believed AI would be a greater asset to cybersecurity teams than threat actors, whereas roughly three-quarters (73%) of generalists felt that AI would do more to help cybersecurity than harm it.

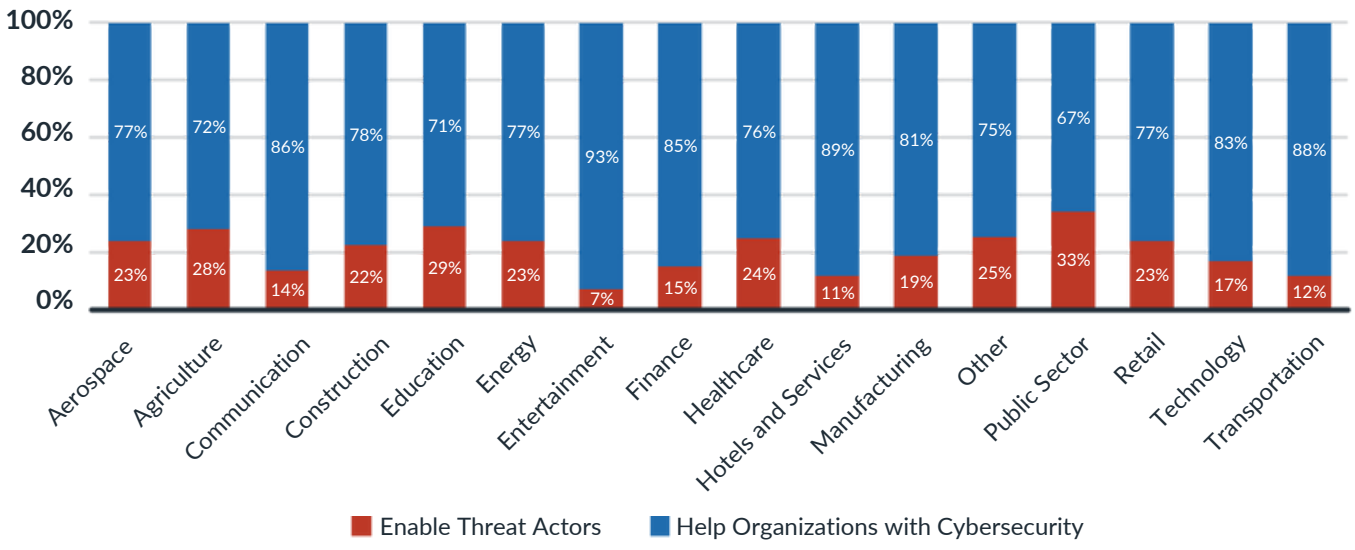
These trends largely repeated by sector, with some slight differences from industry to industry.

Communication, Entertainment, and Hotels/Services were the most optimistic about AI's cybersecurity potential. Agriculture, Education, and Public Sector agencies were the most concerned about AI's cybersecurity impact over the next five years. Their pessimism may be informed by the number of breaches these industries have suffered recently: The Verizon 2024 Data Breach Investigations Report found that the public sector had been attacked more

than other sectors last year, with 12,217 incidents; education was the fifth most attacked sector in their report, with 1,780 incidents.

Respondents were also largely optimistic about AI by country as well. The US stood out as the most pessimistic, with 25% reporting that they felt AI would abet cybercriminals over the next five years.

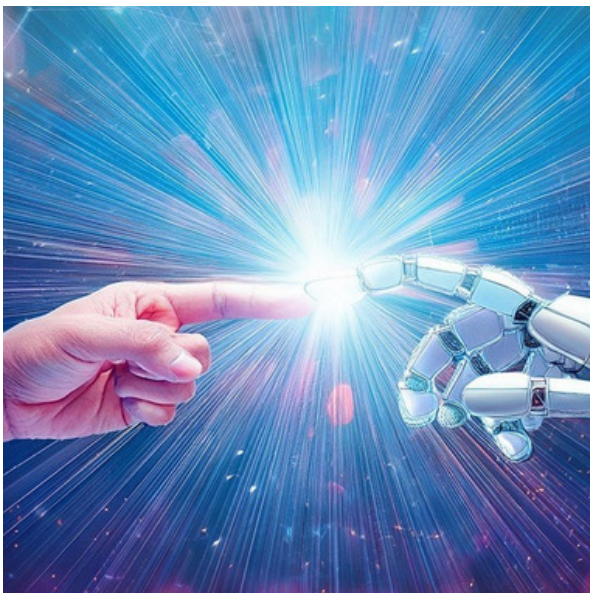
By Sector



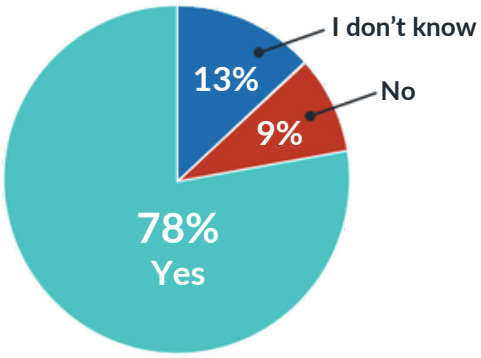
Robots to the rescue

It's not just that respondents feel that AI has potential to help cybersecurity teams—they're also betting on it to do just that. Respondents are putting their money where their mouth is: nearly 4 in 5 (78%) reported that their organization had plans to implement automation, machine learning, or other forms of AI as part of its cybersecurity stack in the next year.

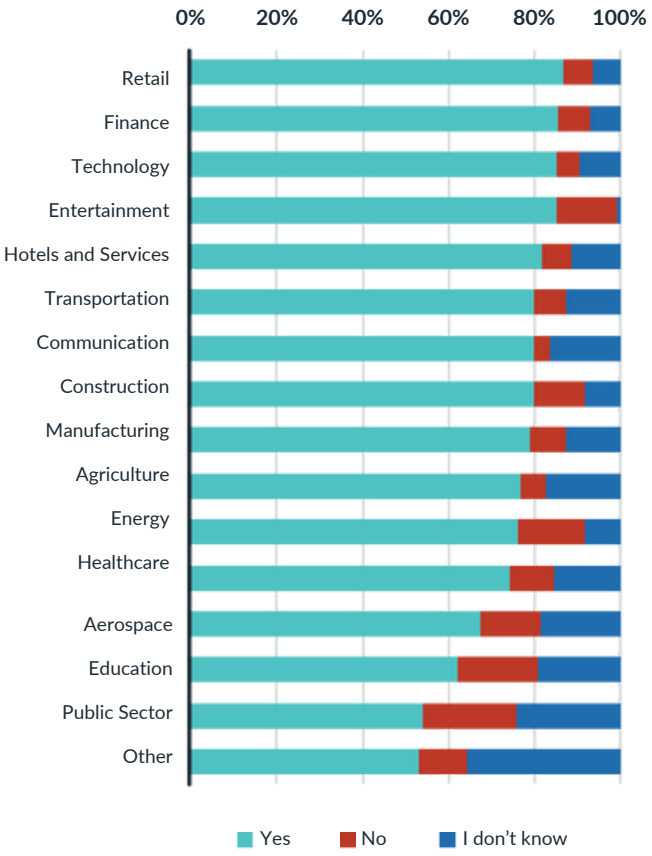
Most respondents in every sector reported that they had plans to implement AI as part of their cybersecurity program. Highly regulated industries were among the sectors that were most likely to indicate that they had plans to invest in AI-powered cybersecurity solutions.



Robots to the Rescue

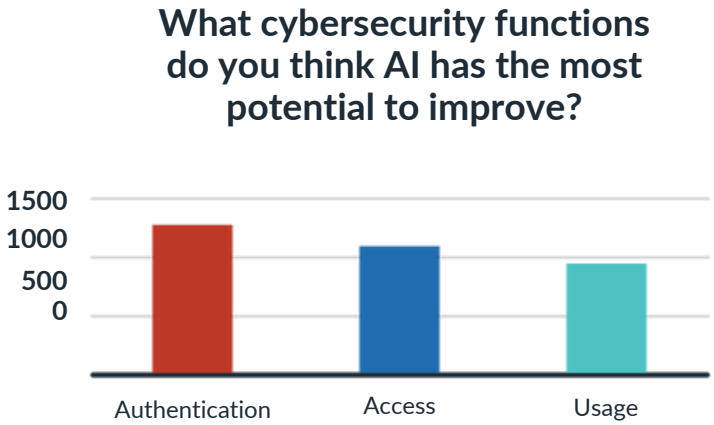


By Sector

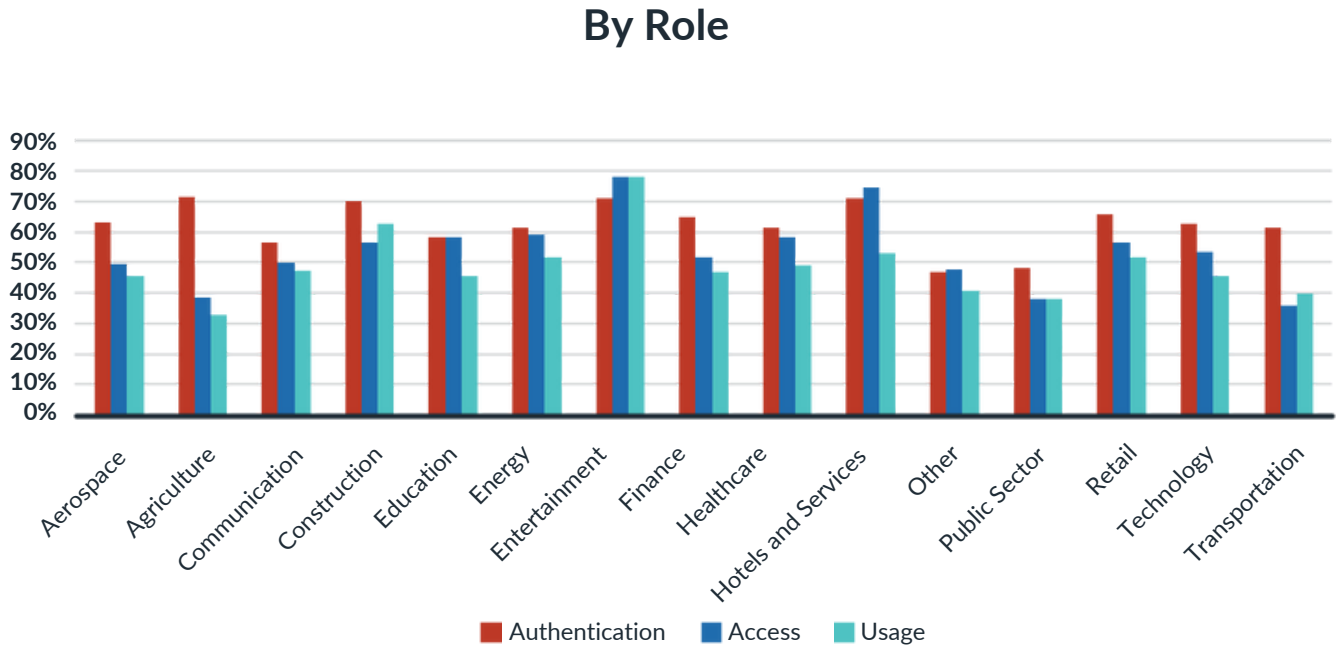


How cybersecurity will use AI

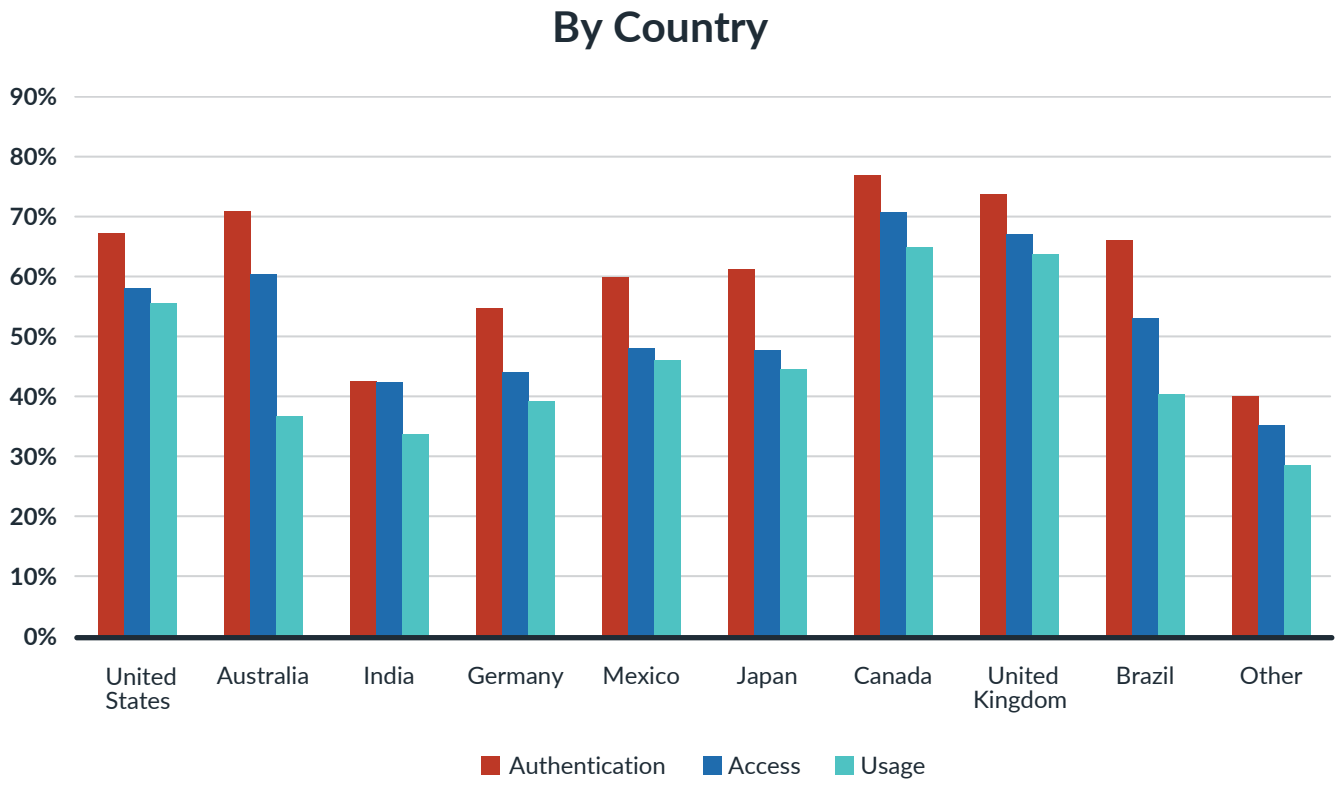
When asked which cybersecurity functions they thought AI has the most potential to improve, respondents most frequently selected authentication, followed by access and usage. Interestingly, only 29% selected all three options, indicating that AI still has a lot of room to grow in peoples' perceptions as a broad security capability.



This pattern tended to recur by both sector and country, with authentication being the top selected choice across all sectors (except Entertainment and Hotels/Services). Respondents working in Construction, Transportation, Entertainment, and the Public Sector selected usage as much as or more often than authentication.



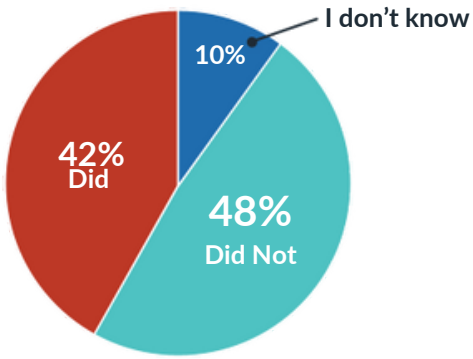
Likewise, authentication was the top choice across all countries. India was the only country where access was chosen as frequently as authentication. Canada, the UK, and Australia had the highest degree of AI optimism by country.



When identity fails, it costs organizations—big.

There's good news and bad news about respondents' answers on data breaches.

"Did your organization experience an identity-related data breach within the last three years?"

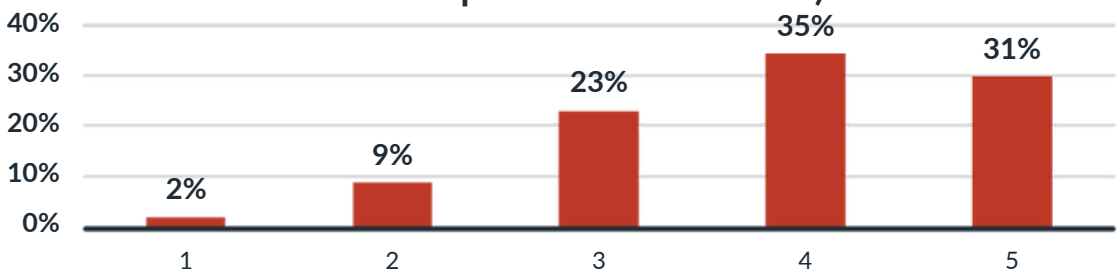


The good news is that they're not an everyday occurrence by any means: 48% of respondents did not suffer an identity-related data breach in the last three years. That said, 42% did suffer an identity-related data breach in that time—and 10% didn't know one way or the other.

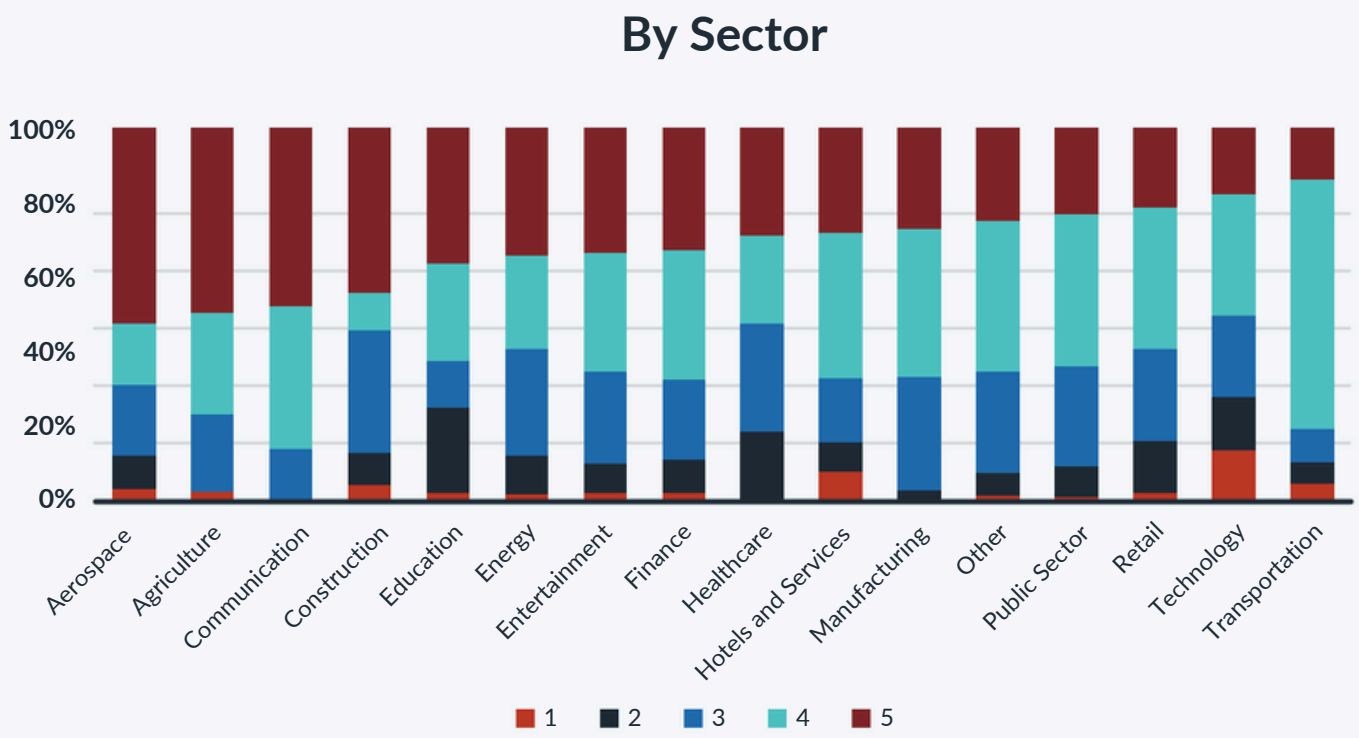
The bad news is that when identity-related data breaches do occur, they have a significant—and costly—impact.

Among organizations that had a data breach, nearly two-thirds (66%) rated it as severe. Experts—especially IAM experts—were more likely to rate these breaches as severe than their cybersecurity or generalist colleagues.

"Rate the severity of the identity-related data breaches your organization experienced over the last three years, from 1 ('The breachers were a non-issue') to 5 ('The breaches caused severe disruption to the business').



This trend recurred across sectors: the majority of respondents rated the severity of a breach at either a 4 or a 5. Aerospace (52%) and agriculture (50%) were the two most likely sectors to rate their breach at a 5. Aerospace was the industry with the highest share of respondents saying their organization had experienced a breach in the last three years, which stands to reason: the more frequently an organization is breached, the more damage those breaches will do.

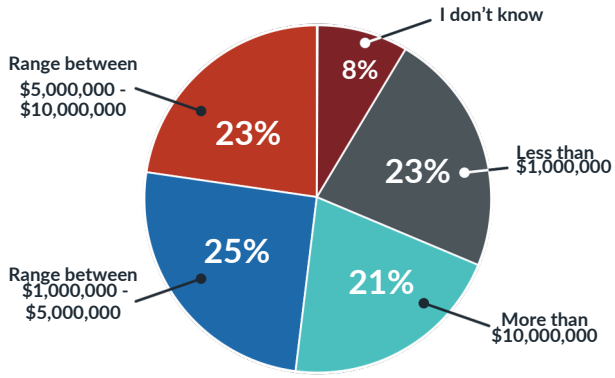


That assessment plays out in the costs that organizations suffered when they were affected by a data breach. When asked to estimate the total remediation, business downtime, and reputational costs that resulted from identity-related data breaches, a quarter of respondents said that total costs would come to between $1,000,000 and $5,000,000.

Nearly one quarter (23%) estimated total identity-related breach costs came to between $5,000,000 and $10,000,000. More than a
fifth of respondents (21%) estimated that total identity-related data breaches exceeded $10,000,000.

Those costs should be alarming, particularly when compared with other reported average data breach costs. The IBM Security Cost of a Data Breach Report 2024 found that the average data breach cost organizations $4.88 million. That average grew by 10% from the $4.45 million average in the 2023 report.

"In looking at your organization over the last three years, how much do you think identity-related breaches have cost your business?"



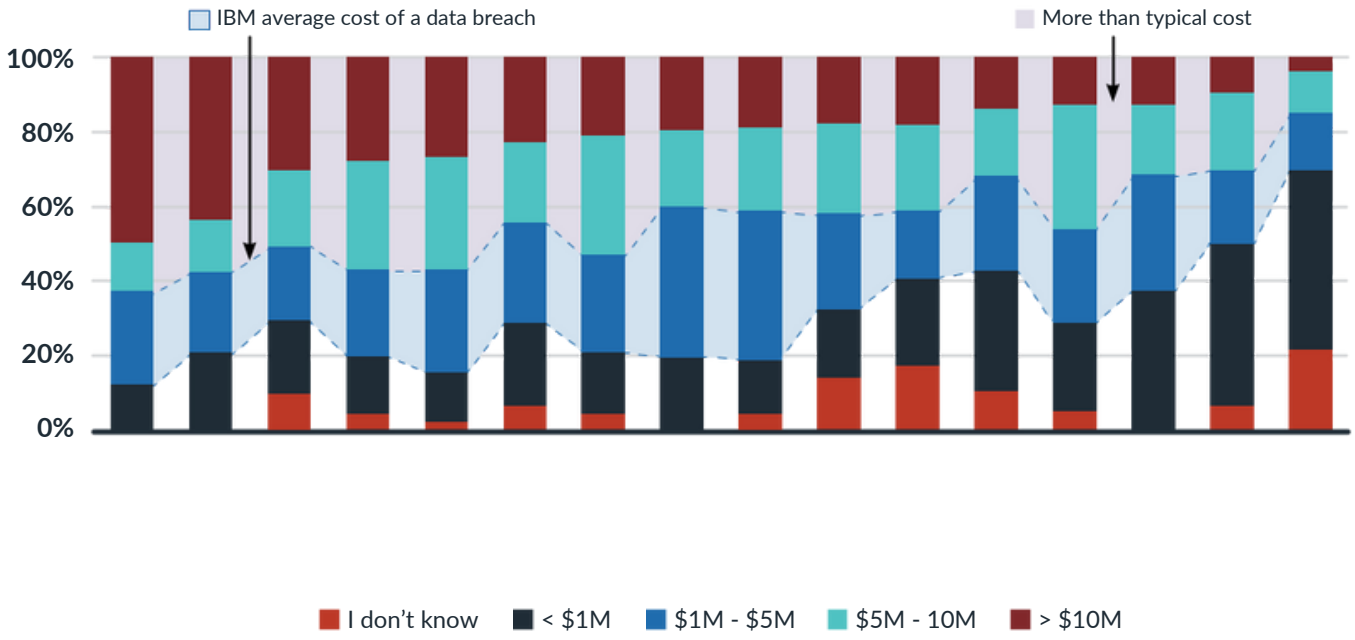
Nearly half (44%) of RSA ID IQ Survey respondents estimated that the cost of an identity-related breach was at least $120,000 more than a general data breach. More than 1 in 5 (21%) estimated that identity-related data breaches cost at least more than double the average cost of a data breach.

By sector, Agriculture and Aerospace estimated that identity-related data breaches tended to cost them the most, with 50% and 43% of respondents noting that breaches had cost them more than $10,000,000 (respectively). But many sectors fared worse (and paid more) when identity was the cause of a data breach: 57% of respondents who work in Construction,

" The takeaway is clear: when identity fails organizations, it costs them big."

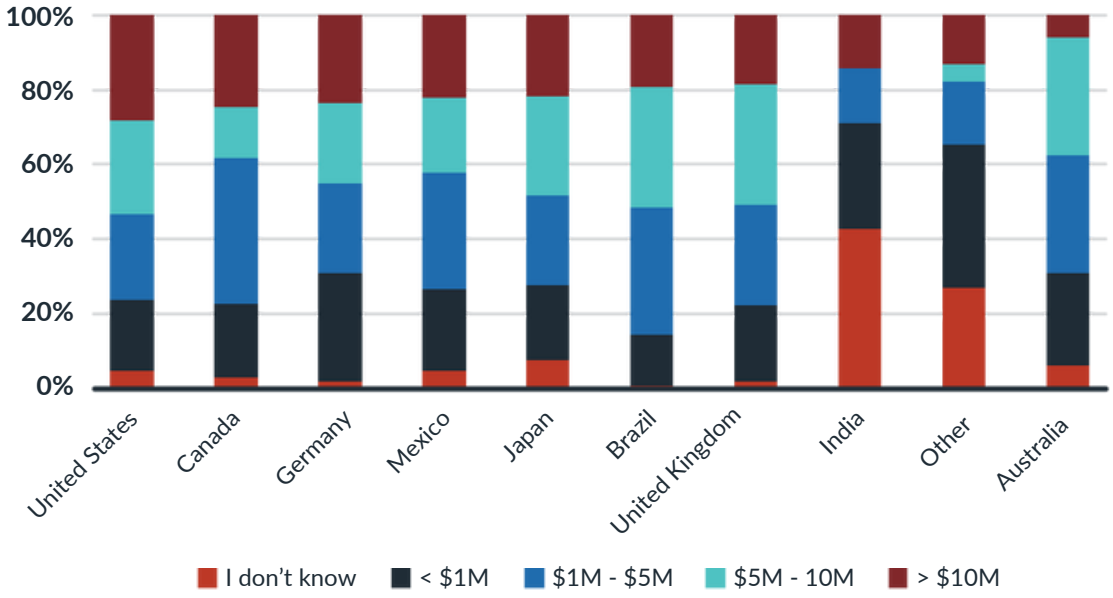
Hotels, and Finance said that an identity-related breach cost them $5,000,000 or more; 53% of respondents who work in Energy said identity-related breaches cost them more than a typical breach.

By Sector



The United States reported the largest share of breaches that exceeded $10 million and among the top countries to rate their data breaches as the most severe.

By Country



Cybersecurity enters its passwordless era.

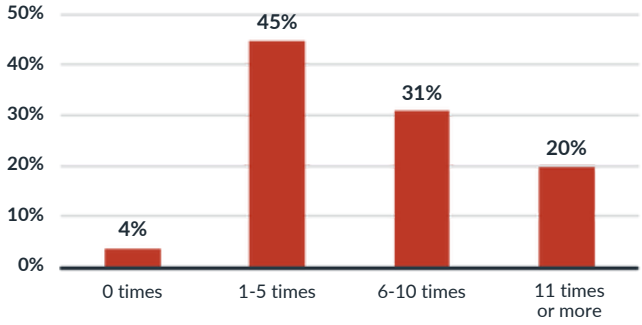
If cybersecurity agrees on anything, it's that passwords are garbage. They're difficult for users to remember, easy for cybercriminals to guess, and costly for IT help desks to manage. They're also a cybersecurity nightmare: most data breaches begin with compromised credentials (or with phishing—which leads to compromised credentials).

Don't take our word for just how unwieldy passwords are. More than half (51%) of respondents had to type in their passwords six times or more every day.
These answers may inform why so many respondents across sectors believed that AI had the most potential to improve authentication.

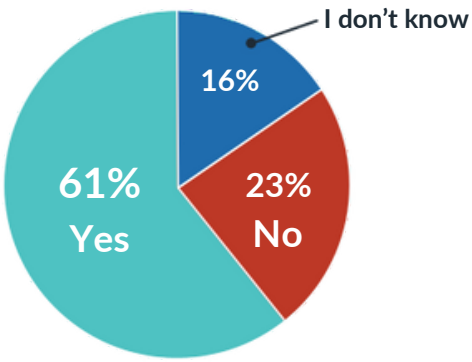
The burden of inputting passwords half a dozen times or more every day seems to have a silver lining: organizations are taking steps to finally get rid of passwords for good. More than 6 in 10 (61%) of respondents said that their organization had plans to implement passwordless authentication in the next year.

That pattern recurred across sectors, with all sectors except the Public Sector and "Other" indicating that they had plans to implement passwordless over the next year.

"On average, how many times a day do you have to type in your password for work?"



"Does your organization have plans to implement passwordless authentication in the next 12 months?"



Passwordless is (finally) ready for enterprise use

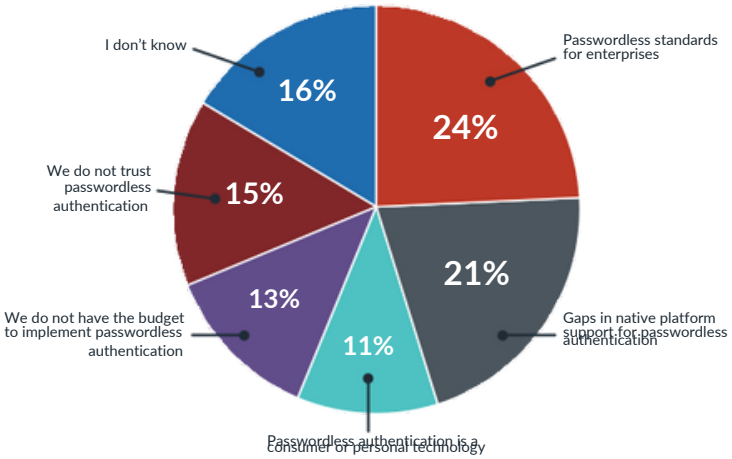
The fact that 61% of organizations are working to implement passwordless authentication in the next year may represent a real push to finally get rid of passwords.

But 61% isn't everyone—nearly a quarter of respondents had no plans to implement passwordless

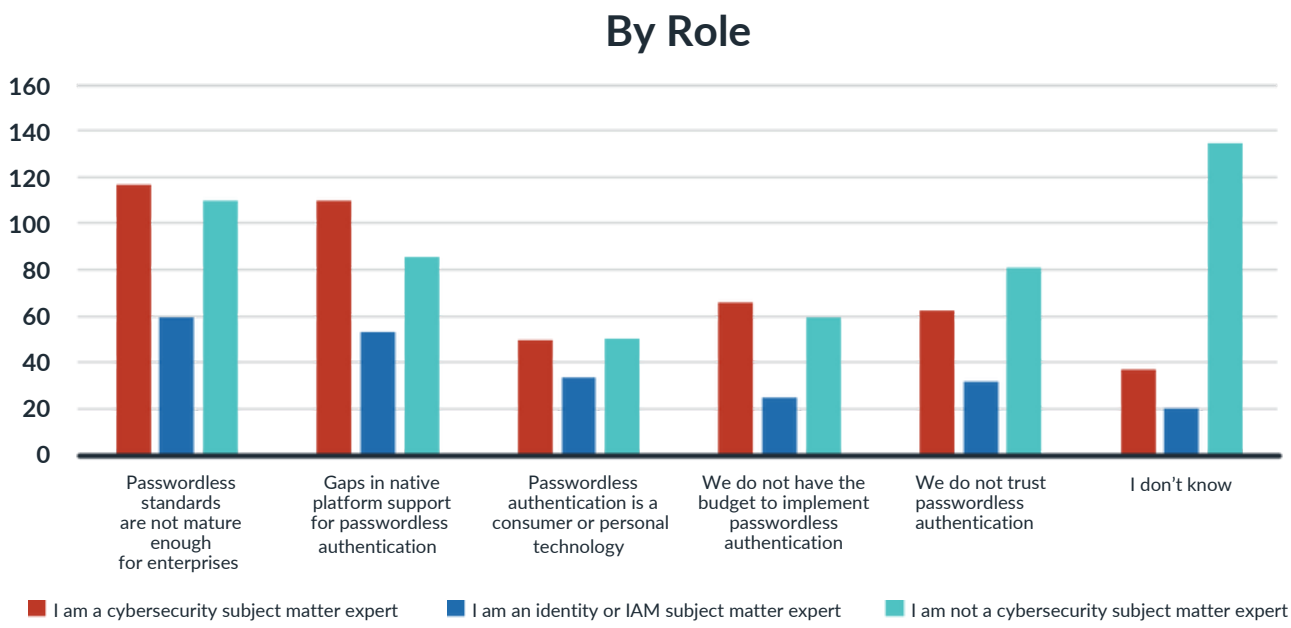
in the next year, and 16% didn't know one way or another. There's also the simple fact that passwords are still involved with the majority of data breaches to underscore just how much work there is left to be done. The Verizon 2024 Data Breach Investigations Report found that the use of stolen credentials was still the top initial action in 24% of data breaches, and that "Over the past 10 years, stolen credentials have appeared in almost one third (31%) of breaches."

We wanted to know why passwords have stuck around for so long or, more specifically, what has prevented or is continuing to prevent organizations from implementing passwordless. The answers revealed real skepticism about passwordless authentication's maturity and applicability for enterprises. Nearly a quarter (24%) felt that passwordless standards were not mature enough for enterprises; more than 1 in 5 (21%) said gaps in native platform support for passwordless were preventing them from using it; 15% said they did not trust passwordless; and 11% felt that passwordless is a consumer or personal technology. Only 13% cited a lack of budget for passwordless authentication as the issue keeping them from implementing the technology.

"What has prevented or is preventing your organization from implementing passwordless authentication? Select all that apply."



There was also a significant difference in responses by role. Cybersecurity experts and generalists were more likely to distrust passwordless authentication than IAM experts. In the 40% of organizations that don't have plans to implement passwordless in the next year, IAM experts may face an internal uphill battle.



Not all passwordless authentication is created equal

There's reason for some skepticism about passwordless technology, particularly in enterprise use cases. That may be due to lingering ambiguity in the market about what a "passkey" really is, and the fact that not all passkeys are appropriate for professional use.

There are now two types of passkeys, as defined by the FIDO Alliance: device-bound and synced.

Device-bound passkeys are generally hosted on specific "'security key'" devices. On a device-bound passkey, key pairs are generated and stored on a single device; moreover, the key material itself never leaves that device.

Synced passkeys save the key material to a remote sync fabric, and the key material can then be restored on any other devices owned by the same user. The current major sync fabrics are Microsoft, Google, and Apple. If a user were to use their Android phone as a passkey, then the corresponding key material would be available on all their other Android devices.

That means that if a synced passkey is compromised on one device, then it's compromised everywhere. That's not a theoretical vulnerability: in 2023, Retool discussed how threat actors had used it to gain access to its systems. Retool wrote that the functionality means that "if your Google account is compromised, so now are your MFA codes."

It's also why RSA uses device-bound passkeys by default (and why RSA prevents the use of synced passkeys by default as well).

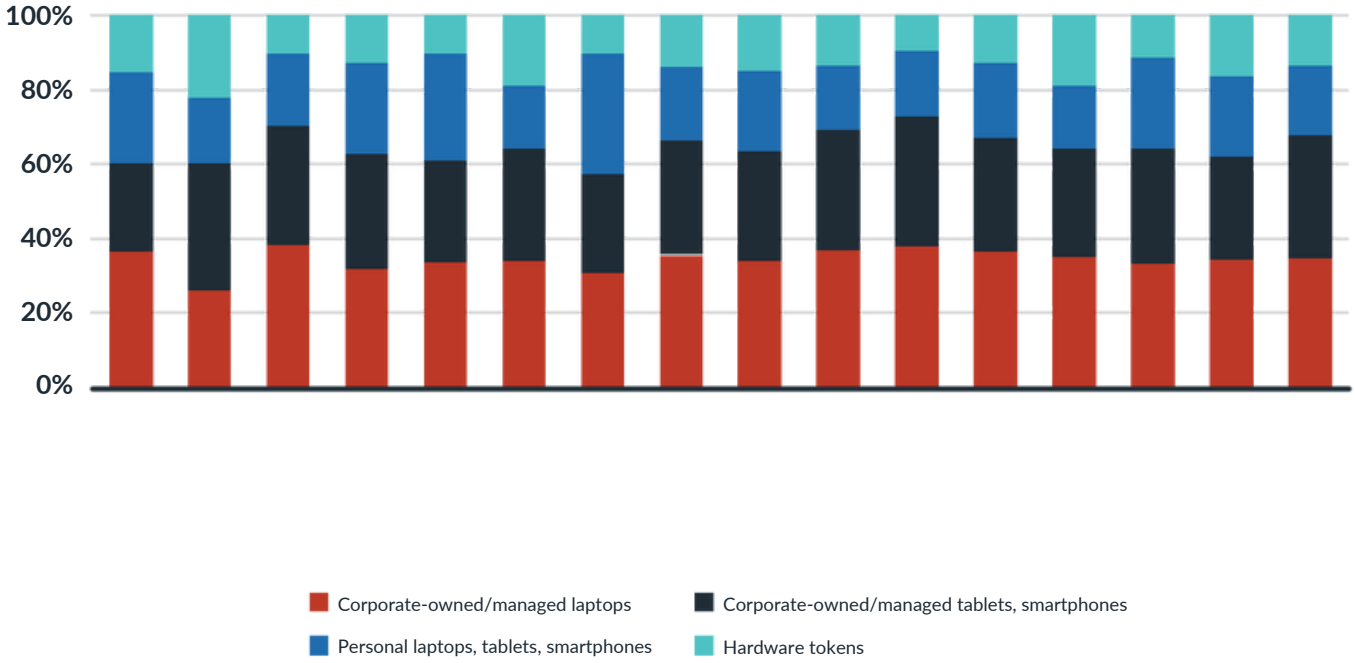
Mind the mobile security gap.

Most respondents noted that they use some combination of corporate-owned devices—including laptops, tablets, phones, and hardware tokens—to fulfill MFA prompts. Roughly 1 in 5 (21%) said they use personal devices. The same was true across industries.

Given that users tend to use professional devices to complete MFA requests, asking hypothetical questions about installing security monitoring on personal devices may be just that. It may also inform respondents' willingness to have their organizations install security monitoring software on their personal devices, with nearly 6 in 10 (59%) claiming they wanted professional monitoring software on their devices.

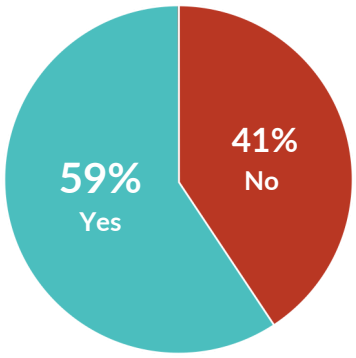
"How does your organization complete MFA requests? Select all that apply."

By Sector

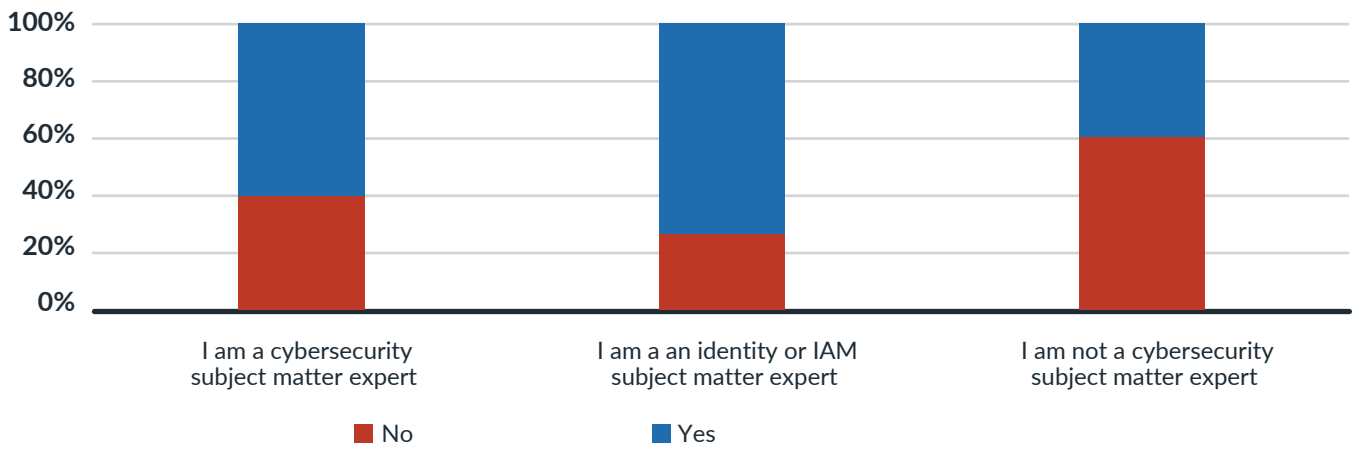


The devil may be in the details: 73% of IAM experts and 60% of cybersecurity experts wanted their organization to install monitoring software on their personal devices. Conversely, only 40% of generalists wanted the same. That's an awful lot of daylight between experts and non-experts; the former may have an uphill battle in convincing the latter to install security software on personal devices. We'd recommend watching out when push comes to shove.

"Do you want your organization to install security monitoring software on your personal device?



By Role



Don’t fly too close to the sun.

We wanted to leave readers with a final thought—and a call to action. Throughout the report, aerospace has encountered the most turbulence of any industry. By sector, it was the most likely to report having suffered an identity-related breach, the most likely to say that breaches caused severe disruption to business, and the second likeliest to say that the costs from identity-related breaches exceeded $10 million (behind agriculture).

We won’t speculate on why. But we’ll also observe that aerospace was the second most likely sector to say they were extremely confident that they could complete an audit in the next month (behind entertainment). Aerospace also had the highest degree of confidence that they could manage all users’ access entitlements.

It’s too simple to say that overconfidence in your identity security stance leads to more frequent, more severe, and costlier data breaches. But it is accurate to admit that identity security—controlling all users, devices, entitlements, and environments—is extremely challenging. Likewise, it’s accurate to say that most successful attacks target weaknesses in identity.

Organizations would do well to remember the scope of that challenge—and to take action to prevent a growing threat landscape from doing them harm.

Learn Why the World's Leaders Are Secured by RSA.

RSA® ID Plus is the world's most secure identity and access management (IAM) platform and provides complete authentication and access capabilities across cloud, hybrid, and on-premises environments. Learn why the world's leaders use ID Plus to secure their users:

Start your free 45-day trial of ID Plus on RSA.com

About RSA

The AI-powered RSA Unified Identity Platform protects the world's most secure organizations from today's and tomorrow's highest-risk cyberattacks. RSA provides the identity intelligence, authentication, access, governance, and lifecycle capabilities needed to prevent threats, secure access, and enable compliance. More than 9,000 security-first organizations trust RSA to manage more than 60 million identities across on-premises, hybrid, and multi-cloud environments.

For additional information, visit our website to contact sales, find a partner, or learn more about RSA.