RSA

RSA.com

# 2023 RSA ID IQ Report

## Human Capability, AI Potential, and the Future of Cybersecurity

OWN YOUR
IDENTITY.

# Table of Contents.


Executive Summary ..... 2

Results and Analysis ..... 5

- Identity is Changing Faster than Users Can Keep Up ..... 6
- Identity Security Demands More than MFA ..... 7
- Users Recycle Passwords More Often than IAM Experts Expect ..... 8
- Unmanaged Devices are Prime Targets for identity Compromise ..... 8
- Fragmented Identity Solutions Drive Up Costs, Slow Down Productivity ..... 9
- Cybersecurity's AI Future ..... 9

# Executive Summary.

Rohit Ghai, CEO, RSA

# Baselining Human Users Before the Advent of AI

Identity is as much the defender's shield as it is the attacker's target. In fact, it is the most consequential part of the attack surface. Identity is first and foremost a security problem.

With exponential growth in the number of human and machine actors on the network, and more sophisticated technology in more places, identity in this new era is rapidly becoming a super-human problem. We need the help of AI technologies to manage all the identities throughout their lifecycle.

Paradoxically, even in this world where AI can dynamically assess risks and automate responses to threats, humans will have an even more important and strategic role in cybersecurity and identity security.

We will need to reinvent ourselves. In time, I don't think we'll be performing day-to-day security operations or sitting in the driver's seat—instead, I think we'll be creating the highways where AI can operate, setting the rules of the road, and establishing the standards that AI needs to meet in order to operate. Whether it's defending AI, training it, setting its policies, or assessing its interpretations, humans will still have a strategic and lasting role driving cybersecurity.

At the same time, AI will need to account for human error, which will remain one of the biggest risks. It's always going to be easier to phish a user than to hack a system.

To prepare for this new era, RSA assessed human users' identity security knowledge, capabilities, and perceptions before the advent of AI. From April through May 2023, more than 2,350 people across more than 90 countries took the 2023 RSA ID IQ Quiz, answering questions on the best ways to prevent phishing, the role that artificial intelligence will play in the future of cybersecurity, why unmanaged BYOD devices represent cybersecurity risks, the components that can move organizations closer to zero trust, and more.

More than **2,350 people** across more than **90 countries** took the **2023 RSA ID IQ Quiz.**



RSA

Their responses were equal parts concerning and consoling.

- Worryingly, nearly half (48%) of all respondents answered at least half the questions incorrectly.
- Almost two-thirds (65%) of self-described identity and access management (IAM) experts did not select the best practice technologies for reducing phishing.
- But nearly all (97%) cybersecurity experts correctly believed that unmanaged devices represented prime targets for identity compromise.

It's clear that users' knowledge gaps have a direct effect on data breaches and other security incidents: the Verizon 2023 Data Breach Investigations Report found that "74% of all breaches include the human element, with people being involved either via Error, Privilege Misuse, Use of stolen credentials or Social Engineering." It's always going to be easier to phish a user than hack a system.

While users' responses indicated that identity security knowledge gaps give cybercriminals an opening, 2023 RSA ID IQ Quiz-takers also gave us some hope: 91% said that AI can perform mission-critical cybersecurity functions, like detecting suspicious access attempts or identifying irregularities in access entitlements. In fact, respondents put an overwhelming degree of trust in technology, with 64% saying that they would trust a computer or password manager to secure their information—and not their partner, closest friend, or financial advisor.

**64%**

**said they'd trust a computer or password manager with their banking information before their partner, closest friend, or financial advisor.**

And most promising of all, the fact that 2,350 people took this test indicates that identity is top-of-mind, a critical cybersecurity component, and simply worth learning more about.

I wholeheartedly agree. That's why RSA will continue sharing future iterations of the RSA ID IQ Quiz and publishing reports that detail users' responses. Because with so much changing, with our roles evolving, and with new risks emerging, we all have a great deal to learn.

*Rohit Ghai, CEO, RSA*

# Results and Analysis.

## Low Knowledge and High Hopes

# Identity is Changing Faster than Users Can Keep Up

Technology is changing rapidly, with growing numbers of users, devices, entitlements, and environments. Meanwhile, the standards and best practices we use to secure those assets are also changing, as are the risks and threats that result from an increasingly large and complex attack surface.

Identity is at the center of each of these trends. It's undergoing massive disruptions faster than most people can track. It's understandable then that 48% of respondents answered at least half of the 2023 RSA ID IQ Quiz's questions incorrectly.

It's also a fact that identity is the most targeted and compromised part of an organization's attack surface. The 2023 Verizon Data Breach Investigations Report found that compromised user credentials "became the most popular entry point for breaches" over the past five years. The Identity Defined Security Alliance found that 84% of organizations reported an identity-related breach in 2022. More than three-quarters of organizations delivering critical infrastructure services suffered an insider-driven cyberthreat in 2022.[1]

Gaps in users' knowledge give threat actors an opening, and there are clear lines between trends in 2023 RSA ID IQ Quiz responses and broader cybersecurity risks. Nearly two-thirds (64%) of all ID IQ Quiz respondents did not select the best practice technologies for reducing phishing; likewise, 65% of self-described identity and access management (IAM) experts did not select the best phishing prevention best practices. Only 57% of respondents selected credential compromise as the most frequent cause of a data breach.

These gaps in users' knowledge give threat actors their favorite vulnerability. Verizon found that phishing is one of the favorite ways that "attackers access an organization." Attackers will usually take the path of least resistance and use what works—more often than not, that means attacking humans and stealing their credentials rather than trying to break the technology that protects them.

[1] *Cybersecurity in Critical National Infrastructure Organizations: 2023. Bridewell. https://www.bridewell.com/us/insights/white-papers/detail/cyber-security-in-critical-national-infrastructure-organizations-2023*

## Low Knowledge Adds Up to High Costs

Because phishing is successful, it makes a major impact on organizations' bottom lines. In its 2022 Cost of a Data Breach Report, IBM found that the "costliest initial attack vector" was phishing, which cost an average of $4.91 million. IBM also found that it took cybersecurity teams an average of 295 days to identify and contain breaches resulting from phishing.

# Identity Security Demands More than MFA

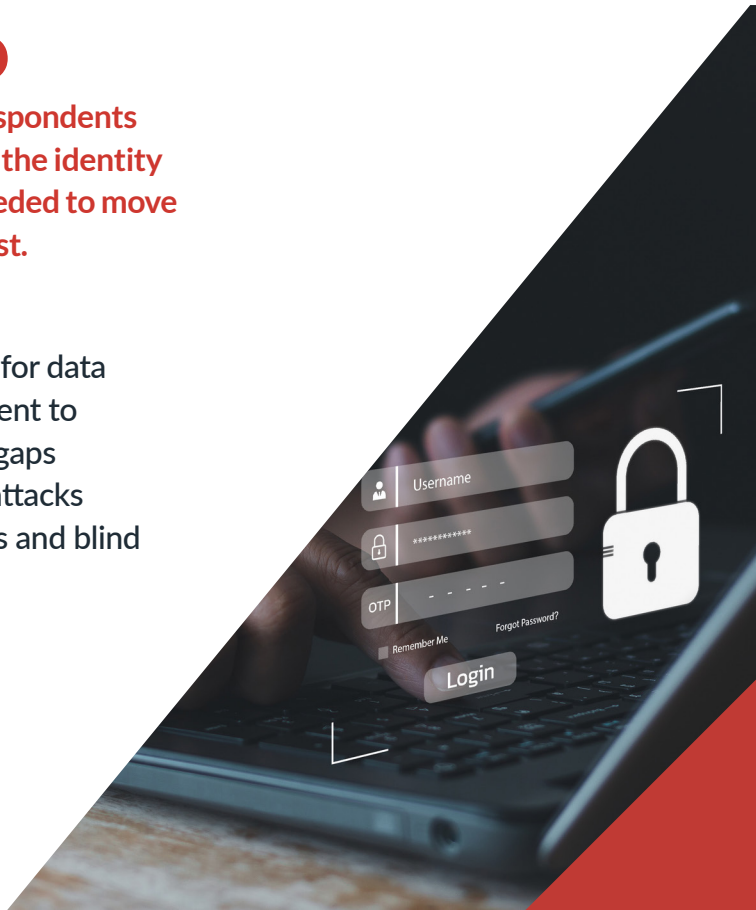
It's not just tactical best practices that flummoxed RSA ID IQ Quiz respondents. Quiz-takers also were stymied by questions about broader cybersecurity strategies: 64% of ID IQ Quiz respondents could not select the identity components needed to move toward zero trust. That's a disappointing performance, especially given the U.S. government's mandate that agencies meet zero trust requirements by the end of Fiscal Year 2024. Identity has a critical role in zero trust. The Cybersecurity Infrastructure Security Agency's (CISA's) Zero Trust Maturity Model lists identity as the first of five pillars that public sector organizations require to move closer to zero trust, noting that agencies need identity security capabilities to "ensure and enforce user and entity access to the right resources at the right time for the right purpose without granting excessive access."

Likewise, more than half of respondents (55%) did not understand the full scope of capabilities—including multi-factor authentication (MFA), single sign-on (SSO), identity governance and administration (IGA), authentication and access controls, and identity threat detection and response—needed to defend against identity threats.

**64%**

**of ID IQ Quiz respondents could not select the identity components needed to move toward zero trust.**

If users don't understand full-spectrum identity security capabilities, or if they don't configure them correctly, then organizations are at risk for data breaches. Look at MFA: it's still the best first line of defense, but on its own MFA is insufficient to defend against modern attacks. In 2022, we saw threat actors evade MFA by targeting the gaps in identity solutions or the misconfigurations between them. These identity infrastructure attacks underscored why organizations need a unified identity platform to remove the identity gaps and blind spots that threat actors exploit.



# Users Recycle Passwords More Often than IAM Experts Expect

Nearly two-thirds (65%) of users admit to recycling the same password across multiple accounts. That's a major cybersecurity risk itself—again, Verizon found that compromised user credentials were the "most popular entry point for breaches" over the last five years.

Bad as that practice itself is, it's made even worse by the fact that the experts who should anticipate that behavior don't know how frequently it occurs. 42% of IAM experts who took the RSA ID IQ Quiz either didn't know or significantly underestimated the frequency with which users admit to recycling their passwords. It's another reason why organizations should find any way possible to reduce their use of passwords and go passwordless.

# Unmanaged Devices are Prime Targets for Identity Compromise

Unmanaged devices have become prime targets for identity compromise: nearly three-quarters of all 2023 RSA ID IQ respondents (72%) believed that people frequently use personal devices to access professional resources. Nearly all (97%) cybersecurity experts believed that threat actors target unmanaged mobile devices.

This aligns with Zimperium's 2023 Global Mobile Threat Report, which found that the average user is 6-10 times more likely to fall for an SMS phishing attack than an email-based attachment.

**97%**

**of cybersecurity experts believed that threat actors target unmanaged mobile devices**

# Fragmented Identity Solutions Drive Up Costs, Slow Down Productivity

Nearly three-quarters of quiz respondents either didn't know or significantly undervalued the cost of a password reset, including nearly half of all self-described IAM experts. With each password reset costing upwards of $70, resets can account for nearly half of all IT help desk costs.[2] The fact that 73% of respondents can't accurately price this expense or understand its impact on IT helpdesk demand could lead to runaway costs, underscoring the value of using one identity solution for both authentication and access.

Quiz results also revealed how inadequate identity governance and administration (IGA) hurts organizational productivity. Nearly one-third (30%) of all respondents reported that they were prevented from accessing the systems needed to do their work at least once a week.

# Cybersecurity's AI Future

The first step in fixing any problem is admitting that there is one. The RSA ID IQ Quiz demonstrates just how widespread that problem has become.

The good news is that cybersecurity professionals have new tools at our disposal—and users want us to leverage them. Nearly two-thirds (64%) of ID IQ Quiz respondents put more trust in technical innovations to maintain their security than they did in their partner, closest friend, or financial advisor.

**91%**

**of ID IQ Quiz respondents agreed that AI has a role to play in improving identity security.**

The responses on AI's cybersecurity potential are even stronger. An overwhelming majority—91% of ID IQ Quiz respondents—agreed that AI has a role to play in improving identity security. Whether it's by flagging irregularities in authentication, authorization, entitlements, or usage, or automating responses to threats, it's clear that AI has a role in the future of cybersecurity and that users expect us to implement it.

[2] *Forgotten your password? Not having one will make you safer, says World Economic Forum. World Economic Forum. https://www.weforum.org/press/2020/01/forgotten-your-password-not-having-one-will-make-you-safer-says-world-economic-forum/*

RSA

## About the 2023 RSA ID IQ Quiz

The 2023 RSA ID IQ Quiz is the first in a planned series of annual industry surveys. This year's survey consisted of 15 questions and was conducted between April and May 2023. The 2023 quiz sampled more than 2,350 respondents from over 90 countries who work across a variety of fields both within and outside of cybersecurity and IAM.

## 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 10,000 security-first organizations trust RSA to manage 59 million workplace identities across on-premises, hybrid, and multi-cloud environments. For more information, go to RSA.com



OWN YOUR IDENTITY.