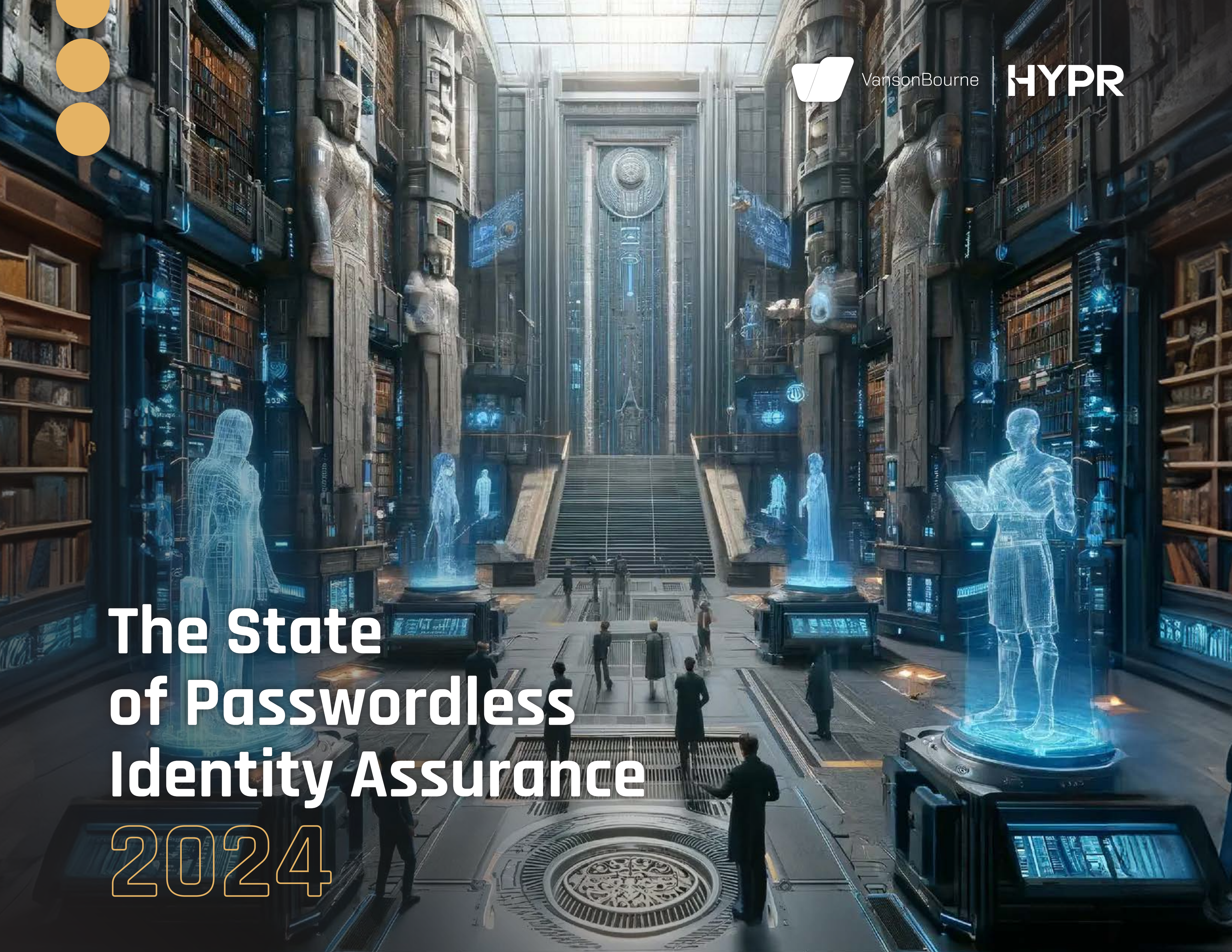


VansonBourne | HYPR

The State of Passwordless Identity Assurance 2024

Contents

Introduction

The fourth annual State of Passwordless Identity Assurance report offers organizational leaders and frontline IT personnel crucial insights into identity threats, technologies and trends, empowering them to steer through one of the most swiftly evolving and mission critical areas of IT and security.

The breakneck pace of digitalization is forcing cybersecurity teams to grapple with unprecedented complexity: sprawling IT environments, a staggering number of user identities, and an ever-expanding attack surface. Compounding these challenges are new regulatory requirements, heightened geopolitical tensions, (including major elections in several parts of the world), and the looming threat of AI-powered cyberattacks.

Current identity security structures are ill-equipped to handle this new normal, which requires a more holistic approach. CISOs, aware of these deficiencies, are turning their attention to overhauling their identity security frameworks. In a recent survey, the User Access/IAM category moved into the top position of CISOs security priorities and investment areas for the first time.[1]

The recent onslaught of high-stakes breaches only underscores the urgency. The attack on MGM Resorts in September 2023 began with, fraudsters convincing service desk personnel to reset an employee's credentials to grant them access. This lead to them eventually gaining control of the entire system and a collective loss of $100 million. And this February, a multinational finance firm lost $25 million in one fell swoop when attackers used deepfake video and audio to impersonate executives and trick an employee into transferring the funds.

With identity front and center for attackers and security teams alike, where should organizations be focusing their efforts? What are the greatest identity security risks and challenges? What steps are they currently taking in response and how successful are these tactics?

The 2024 report delves into these issues and more. As reflected in the new name, "The State of Passwordless Identity Assurance," we have expanded the scope of research beyond authentication to encompass the broader identity security field. By taking a wider lens to critical identity security issues and trends, we aim to better arm teams in building future-ready approaches and strategies.

The research and analysis – conducted independently by Vanson Bourne and sponsored by HYPR – is based on interviews of 750 IT security decision makers with knowledge and/or responsibility for cybersecurity. These IT security decision makers were from organizations in EMEA, Asia-Pacific and Japan (APJ) and the US, ranging in size from under 100 employees to over 5,000.

Key Findings

91%
of breached organizations name credential misuse or authentication weaknesses as a root cause

$5.48m
average cost of authentication-related breaches in the last 12 months

$2.78m
average cost of identity fraud over the last 12 months

29%
of IT helpdesk spend is attributed to password issues

68%
of employees wait up to 3 hours for service desks to verify their identity

75%
expect AI to give them an advantage over cybercriminals

60%
name generative AI as their biggest identity security concern

86%
say that the increased number of cyberattacks as a result of upcoming elections is among their biggest concerns

89%
believe that passwordless authentication provides the highest level of security

Threat Trends and Impacts

1

Identity Security Cracks Leave Organizations Exposed

Identity-focused attacks remain the most vulnerable entry point into an organization. With billions of compromised credentials readily available on the Dark Web, cybercriminals can simply exploit legitimate accounts to infiltrate systems and exfiltrate data. The Cybersecurity and Infrastructure Security Agency (CISA), the National Security Agency (NSA), the UK National Cyber Security Centre (NCSC) and other security bodies continue to advise that organizations shore up their identity security controls, emphasizing phishing-resistant authentication in particular.[2]

Our research bears this out. Nearly eight in ten (78%) organizations experienced an identity-related cyberattack in the last 12 months — but it was those from industries containing high-value data that were particularly susceptible, including those from financial services (86%) and legal (85%). Phishing (39%) continues to be among one of the most prevalent forms of attack, as does identity impersonation (28%) and push notification attacks (26%). Push notification attacks (also known as MFA prompt bombing or MFA fatigue attacks) were practically unheard of 3 years ago, accounting for only 9% of attacks in our 2021 report. Today they are a staple of the hacker's toolkit, used in several major attacks including a recent scam targeting Apple users.[3]

Types of Cyberattacks Faced in the Last 12 Months

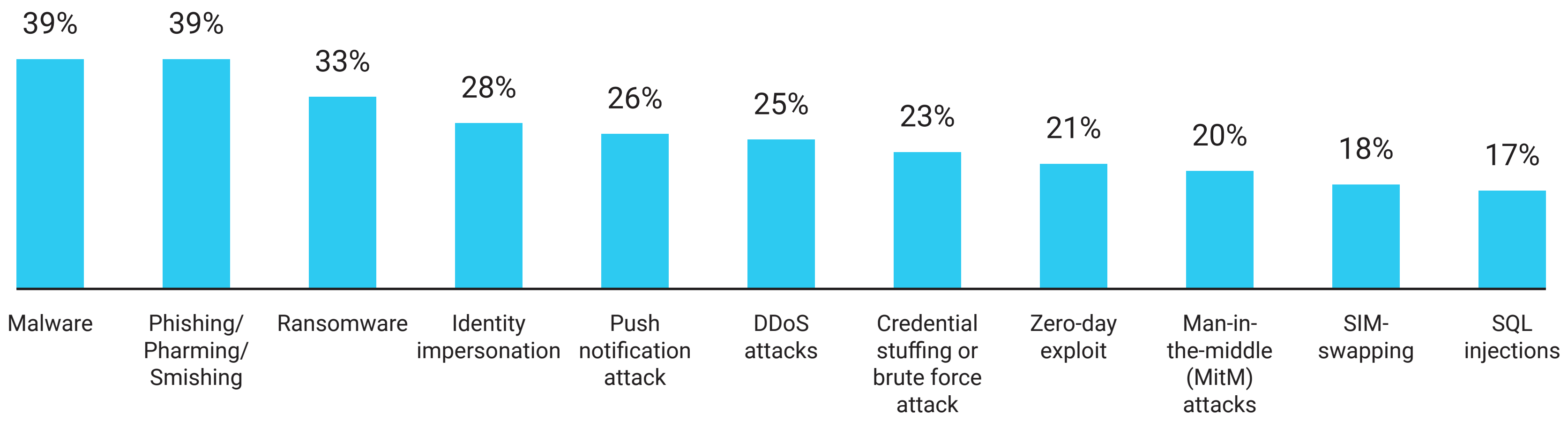


Figure 1: What, if any, types of cyber-attack has your organization faced in the last 12 months? [750], omitting some answer options

Not surprisingly, the vast majority (84%) of organizations hit by a cyberattack went on to experience a breach. Further, over six in ten (62%) suffered multiple breaches.

These statistics indicate that the majority of organizations are not yet heeding industry and governmental guidance on identity security, leaving their identity processes and end users vulnerable to attack. More than nine in ten (91%) of organizations that were breached name credential misuse or authentication weaknesses as a root cause, a notable rise from 82% the previous year. If looking across all surveyed, this indicates that more than two-thirds (69%) were breached through their authentication processes. It is famously said that hackers don't break in, they log in.

Insecure devices and outdated devices are another likely contributing factor. An analysis of anonymized data collected by the HYPR platform[4] revealed that, for users of the iPhone platform, 21% of employees are using devices that were released in 2019 or earlier with outdated operating systems.

Identity fraud is another glaring area of vulnerability for organizations. Fraudsters continually develop new and sophisticated ways of stealing identities and circumventing common identity verification controls. The vast majority of organizations (78%) admit that they have been a victim of identity fraud within the last 12 months. In fact, identity verification issues plague organizations on multiple fronts, which we explore in more detail later in this report.

91%
of organizations that were breached name credential misuse or authentication weaknesses as a root cause

78%
of organizations admit they were a victim of identity fraud

Top Business Impacts

Identifying and responding to a cyberattack is only the first step; organizations must also navigate the fallout – which is often far-reaching and multi-faceted.

Nearly all (85%) of the organizations that experienced a cyber breach in the last 12 months sustained negative impacts to their business.

Over a third (34%) lost customers to a competitor and even more admitted that sensitive data was lost or stolen (35%). Other top impacts included incurring fines (32%) and reputational damage (32%).

Impacts of Cyber-Breaches

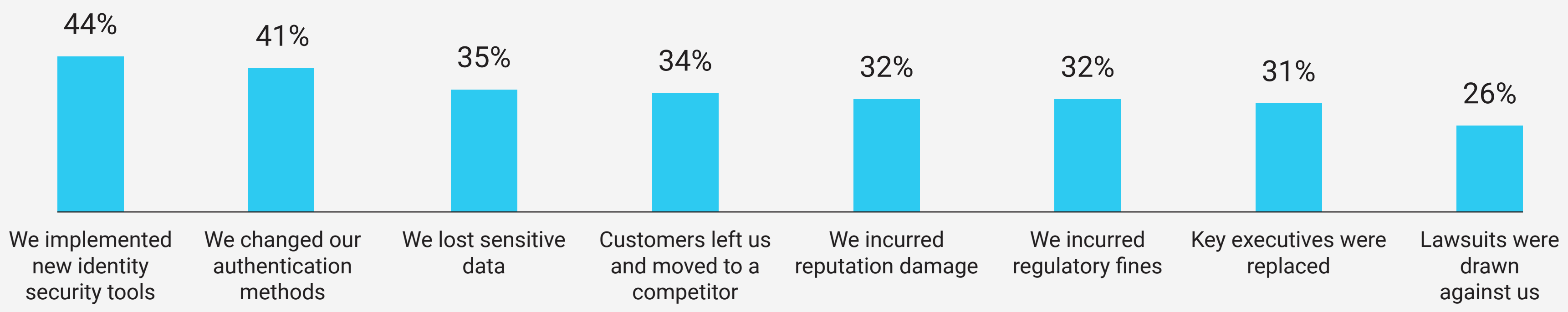


Figure 2: What was the impact of the cyber-breach(es) that your organization experienced in the last 12 months? Only asked to those from organizations that had experienced a cyber-breach in the last 12 months [571], omitting some answer options

What steps are organizations taking in response? Encouragingly, around two-thirds (67%) implemented new identity tools and/or changed their authentication methods as a result. While the effectiveness of these measures remains to be seen, this represents a welcome focus on identity defense. Of course, this also reveals the concerning fact that one-third (33%) of organizations took no action after a breach.

Quantifying the Impact

While it can be tough to calculate the true cost of a breach, organizations are reporting sizable hits to their bottom line. On average, cyber breaches caused by insecure authentication cost organizations a hefty $5.48 million in the last 12 months – a considerable rise from $2.95 million the previous year. The financial implications have been especially severe for those in the energy and legal industries with each facing average costs of $6.45 million and $6.41 million respectively. By contrast, healthcare losses from authentication-related breaches were over a third less, at an average of $4.12 million.

$5.48m

average cost of authentication-related breaches in the last 12 months

This doesn't include the toll from identity fraud. Identity fraud is so rampant that well over half of organizations (58%) fell victim multiple times within the last 12 months, costing them a further $2.78 million, on average.

As high as these numbers may seem, they're unlikely to be the conclusive figures. Organizations can expect additional, delayed financial consequences due to lost business, long-term remediation work, cyber insurance premium increases or reputational damage. Lawsuits are also common, impacting around a quarter (26%) of organizations.

Organizations' Existing Identity Platforms Fall Short

We've seen significant and ongoing consolidation in the identity security market in recent years. Identity and access management (IAM) platforms are merging and/or acquiring identity security tool companies, privileged access management (PAM) providers are acquiring identity threat detection and response (ITDR) and identity governance and administration (IGA) providers, and IGA providers are remaking themselves as IAM platforms. In doing so, they hope to provide integrated solutions with broad identity management and security capabilities. In practice, however, it doesn't appear this approach is yet translating into a tangible advantage for their customers.

In fact, the majority of organizations felt compelled to either switch platform vendors and/or purchase a point solution from a newly sourced vendor when looking to improve their identity security after a breach.

Switched Platform Vendor and/or Purchased a Point Solution From a New Vendor After a Breach

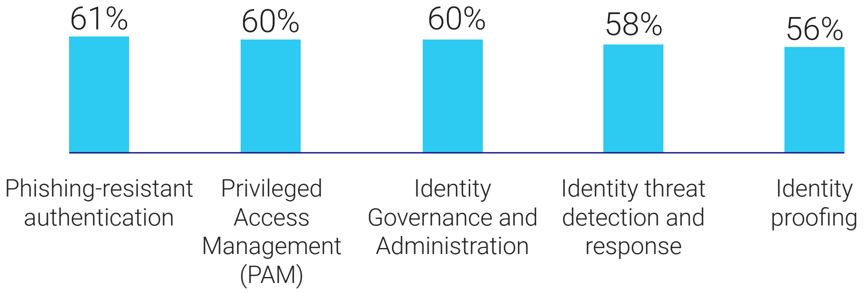


Figure 3: As a result of experiencing a cyber-breach, which of the following steps, if any, did your organization take towards the following aspects of identity security? [571] Only asked to those from organizations that have experienced a cyber-breach in the last 12 months

Ongoing Identity Security Challenges

2

Shifting to Identity-First Security

Historically, identity and access management focused on controlling insider access, relying primarily on perimeter-based security systems to thwart cyberthreats. However, even before the Covid-19 pandemic, organizations were rushing toward digitalization, migrating critical data and workloads to the cloud and rendering the traditional security paradigm obsolete.

Today, identity is the new perimeter. HYPR data shows that 63% of employees login from multiple IP addresses, with 30% logging in from four or more places.[5] Unfortunately, security controls have lagged behind this identity-centric reality. The overwhelming majority (99%) of organizations remain tethered to legacy authentication methods with limited security, with over half using traditional multi-factor authentication (55%), username and passwords (53%) and/or biometrics that retrieve a password (51%).

Encouragingly though, IT security decision makers are well aware of the gaps in their organization's defense. Around half (52%) admit that their organization's approach to authentication is not completely secure, with almost four in ten (37%) stating that their current authentication methods are vulnerable to phishing and credential attacks. An even higher proportion are not fully confident in their organization's ability to detect potential breaches (56%) or mitigate these threats (58%).

The growing acknowledgement that identity is central to cybersecurity marks a pivotal change in the way organizations approach digital threats. We explore how this shift translates into cybersecurity strategies and plans in the final sections of this report.

53%

still use only a password to protect access to some systems

The Explosion in Digital Identities

In an environment where cybercriminals eagerly exploit any weakness, the rapid growth in digital identities is placing enormous strain on IT and security systems. Nearly all (99%) IT security decision makers report an increase in the number of digital identities used by their organizations' employees. Much of this growth arises from the spreading digitalization of the workplace. Approaching half (45%) of organizations report that the adoption of new technologies and applications are behind the rise in identities, with a similar number citing an increase in employees using new technologies (43%). Remote work was called out by 35% of organizations — a reminder that remote identity access has become a permanent fixture, despite the return to office by some.

Factors Driving Digital Identity Growth

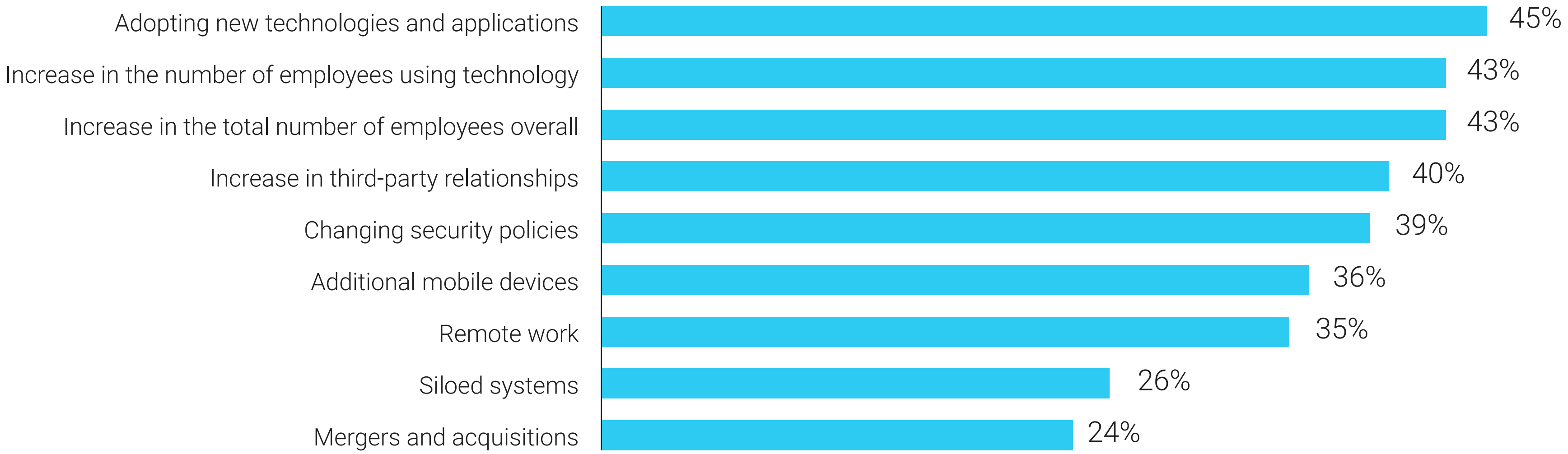


Figure 4: What factors, if any, are driving the number of digital identities used by your organization's employees to access platforms, applications and systems? [750]

It's unsurprising that nearly all organizations (98%) voice frustration over current identity security methods, with challenges seen across the business. The complexity to deploy and/or manage these methods was the top pain point, further exacerbated by the growing number of digital identities. Similarly, securing remote and offline workers is still a minefield for many (29%). A large number of difficulties center around the user experience, which we look at more closely in the next section.

Pain Points Associated With Current Identity Security Methods

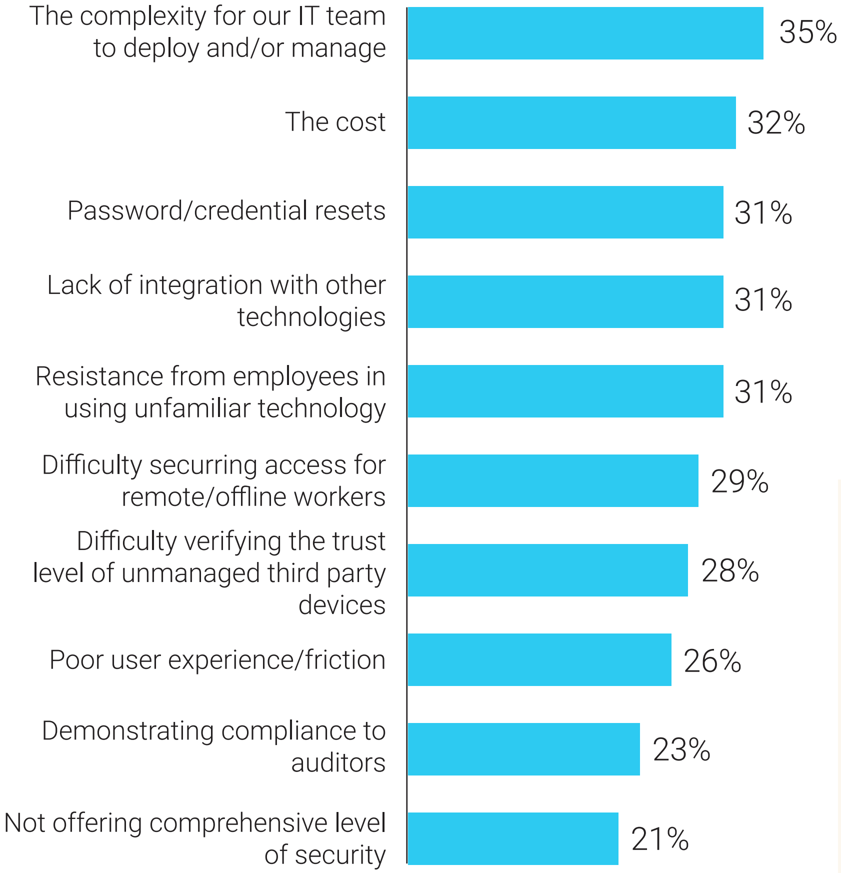


Figure 5: What are the pain points associated with your organization's current identity security methods? Combination of responses ranked first, second and third [750]

Current Identity Security Practices Drain Time and Resources

User experience plays a pivotal role in the effectiveness of identity security solutions; even the most robust solution becomes ineffective if employees struggle or refuse to use it. Unfortunately, user experience is an ongoing complaint for the majority of organizations. Nearly a third report that employees resist using unfamiliar technology (31%), and the same number point to issues with password/credential resets.

Users also grapple with the sheer variety of authentication methods used on a daily basis — four on average, and 13% use six or more. This means multiple, varying sign-on requirements that employees must navigate, adding even more friction and frustration.

Paint Points are Impacting Multiple Areas

71%
IT-related

69%
UX related

62%
Security related

Passwords are a Pain for Everyone

Password and credential resets don't just affect user experience, they also impact IT teams.

Organizations are spending 29% of their annual IT help desk budget on password-related issues, on average.

Real-Time Verification a Real Challenge

One of the biggest identity security gaps in the workplace involves identity verification processes. Traditionally, identity verification was primarily invoked during employee onboarding and rarely otherwise. The rise in identity fraud and identity-targeted attacks, however, have made ongoing verification a necessity. Unfortunately, organizations are struggling to put effective and efficient methods in place, and name employee identity proofing/verification as one of their top security challenges (37%).

In particular, real-time verification eludes most organizations. Fewer than a third (31%) are able to verify employee identities in under an hour, and a considerable number (20%) take four hours or longer. In fact, most employees are not even sure how to begin the process, spending an average of 21 minutes just to find their respective service desk.

37%

of organizations name identity verification as a top security challenge

58%

take an hour or more to verify employee identities

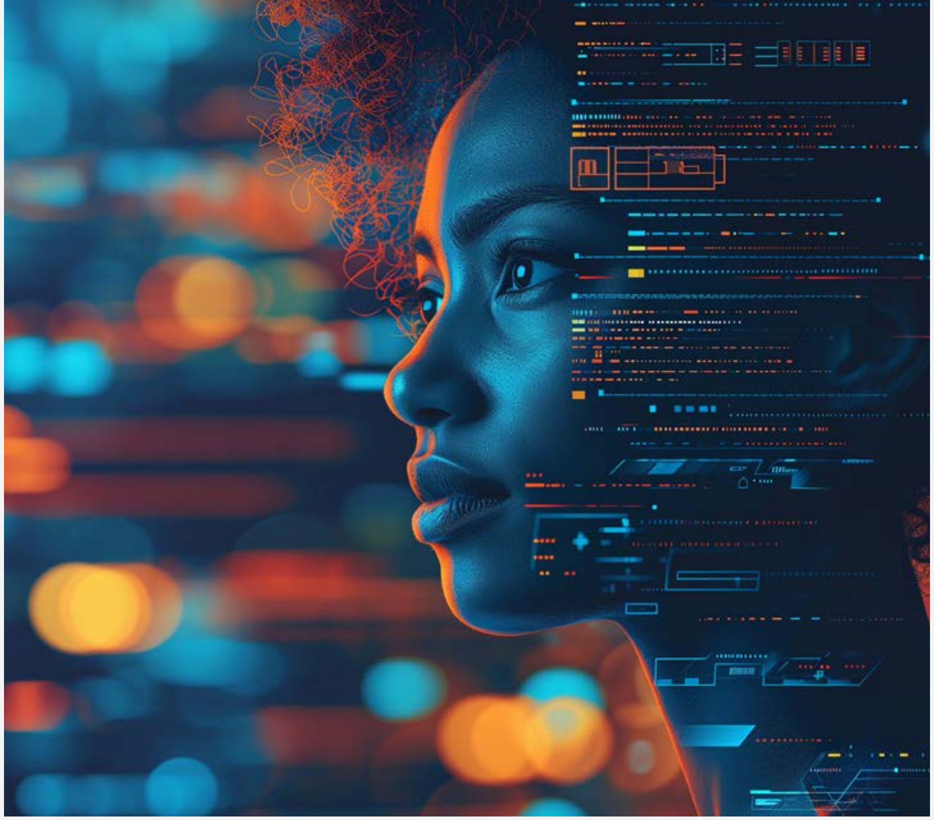
Navigating Tomorrow's Risks

3

Artificial Intelligence Poses a Significant Threat to Identity Security

Artificial Intelligence (AI) presents a double-edged sword for identity security. On one hand, AI can enhance identity security protocols by strengthening adaptive and risk-based controls. On the other, it puts unprecedented power into the hands of both skilled and amateur attackers. Cybercriminals are now wielding AI to exploit vulnerabilities at a relentless pace. With AI, malicious actors can scrape social media and news sites to individually tailor phishing messages, while generating deepfakes so convincing that victims willingly surrender sensitive information or reset credentials.

IT security decision makers are acutely aware of what's on the horizon, naming the increased threat of generative AI (60%) and deepfake identity fraud (45%) among their biggest identity threat concerns over the next 12 months.



Organizations Face Growing Regulatory and Accountability Pressures

As we've seen, cybersecurity strategies are undergoing a shift, with identity security assuming a more central place. Escalating identity-related breaches and emerging threats targeting identity account for some of this realignment, but our research indicates there are other factors driving the focus on modernizing identity security.

Multiple security and data privacy regulations are forcing organizations to tighten their identity security provisions to reflect the new threat landscape. The earlier mentioned guidance from CISA, urging all organizations to adopt phishing-resistant MFA, is just a sliver of the full scope. Enforceable regulations, such as the New York Department of Financial Services Cybersecurity regulations, Payment Card Industry Data Security Standard and the Federal Trade Commission Safeguards rule, are strengthening their requirements, with hefty penalties and fines for non-compliance.

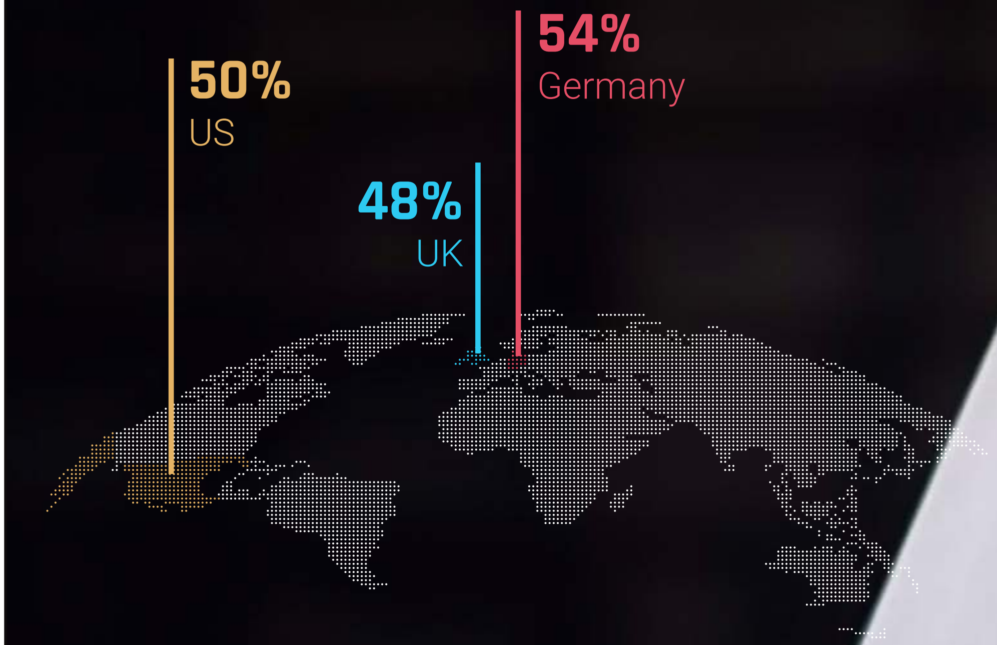
Achieving this compliance, however, is proving a challenge. Organizations cite integration difficulties (39%), deployment struggles (37%) and limited resources for training end users (37%) as passwordless authentication adoption barriers; which in turn makes it harder to meet regulatory mandates. Moreover, around a quarter (23%) report that demonstrating compliance to auditors is a pain point when it comes to their current identity security methods.

Individuals are also increasingly being held accountable for cyber breaches, highlighting a shift towards personal responsibility. New US Securities and Exchange Commission (SEC) guidelines on cyber transparency have raised the stakes for CISOs and boards, requiring faster breach disclosure and mandatory annual reporting on cybersecurity posture and risk. Organizations are also taking active measures to hold individuals accountable for cybersecurity failures, with around a third (31%) replacing key executives as a result of cyber breaches in the last 12 months.

Upcoming Elections in Many Nations are a Major Concern

More than 1.5 billion people from across 64 countries will head to the polls in 2024. Elections often result in heightened cybercriminal activity, including targeted attacks and misinformation campaigns, as various actors attempt to influence outcomes and profit from an environment of sharpened tensions. Security leaders are wary of the repercussions for their organization's identity security. Nearly half (49%) say that the increased number of cyberattacks as a result of upcoming elections is among their biggest concerns. Not surprising that those from countries with upcoming 2024 elections, e.g. Germany, the US and UK, are more likely to cite this as a concern (54%, 50% and 48% respectively).

An increased number of cyber-attacks as a result of elections is major concern, especially among those with elections this year



Toward Identity-First Security

4

The Power of Passwordless Authentication

Passwordless authentication emerges as a critical advancement in the realm of identity security, offering an un-phishable and seamless alternative to traditional, insecure password-based methods. The technology not only strengthens an organization's security posture against cyberattacks, it also streamlines operational efficiency, making it a compelling solution for modern cybersecurity challenges – and IT decision makers recognize this.

Around nine in ten agree that organizations need to embrace passwordless to both ensure user satisfaction (88%) and provide the highest level of security (89%). Furthermore, they are putting this belief into action, with around four in ten (41%) intending to either adopt or continue to use this technology in the next 1-3 years. Interestingly the energy industry, not usually seen as cutting edge, is most inclined to adopt this approach (48%), perhaps a direct result of the significant breach costs they've incurred.

There are various forms of passwordless authentication, with some more secure than others. Passkeys are a form of passwordless authentication based on FIDO (Fast IDentity Online) standards. They replace passwords with a cryptographic key pair and on-device authentication. Nearly all (97%) of the organizations that plan to use passwordless, state they will incorporate the use of passkeys to some extent.

But while the drive to go passwordless is clearly there, is it realistic to expect that this can be achieved quickly?

89%

state passwordless authentication provides the highest level of authentication security

88%

agree that organizations need to fully embrace passwordless authentication to ensure user satisfaction

97%

of those planning to use passwordless authentication intend to incorporate passkeys to some extent

Passkeys: the Gap Between Theory and Adoption

While there may be buy-in for passkeys, indicators suggest it will be some time before organizations replace their passwords with this technology. More than half (53%) still have systems that use only usernames/passwords and 47% will continue to do so for at least the next 3 years.

Part of the barrier may stem from implementation complexities. Nearly one third (31%) name implementing passkeys as a primary identity security challenge for their organization.
Cost may be a further deterrence. Respondents report that implementation costs are the top barrier to their organization adopting passwordless technology (45%). Clearly widespread passkey uptake will depend on the ability of IT teams to overcome their real or perceived implementation problems.

31%

Nearly one third name implementing passkeys as a primary identity security challenge for their organization

A Full-Scale Identity Security Approach

While phishing-resistant authentication is critical, it takes a comprehensive approach to secure identities. According to our research, organizations plan to tackle their identity risks on multiple fronts, with several initiatives on their priority lists, including:

Identity Verification

Given the challenges around verifying employee identities in real time, it's reassuring to see that 43% are very likely to add identity proofing technologies over the next 12 months. This is particularly true of those from the legal industry (56%), where organizations handle highly sensitive data and must adhere to strict compliance regulations.

Risk Policy and Orchestration

Fewer organizations (39%) plan to add to their risk policy and orchestration capabilities. This is concerning given 56% of organizations are not fully confident in their ability to detect a breach.

Artificial Intelligence

Despite concerns over the threats of artificial intelligence, respondents are taking an optimistic view of AI in the long run. Three quarters (75%) believe that, ultimately, their organization will gain an advantage over cybercriminals by adopting artificial intelligence within their identity security stack.

Expanded Training

Human insight and vigilance are essential to any effective security strategy. Recognizing that investing in the human factor is critical, about half of organizations (49%) are very likely to expand cybersecurity training programs over the next 12 months.

Conclusion

As this research makes evident, transformations in both the threat landscape and enterprise IT environments have far outpaced their identity defenses. This is creating serious consequences for security, digital modernization, productivity and growth.

It's not that security teams have been complacent — respondents report taking proactive measures to onboard new identity security tools. Yet their overall, traditional identity models have been left largely intact. The result is a disjointed and dysfunctional patchwork of vendor-dictated, vertically integrated technologies that leave gaps for attackers to exploit.

There are signals of a shift however; increasing calls for a more holistic identity framework. Such a framework rests on phishing-resistant authentication (including passkeys), ongoing identity verification, and the continual assessment and mitigation of identity risks. Taking an integrated, unified approach promises to not only address current and evolving security risks, but also alleviate pain points such as user friction, productivity obstacles and regulatory pressures.

Constructing a Holistic Identity Security Framework

How can companies connect their fragmented identity systems to create a more unified approach? While there's no silver bullet, there are clear, surmountable paths forward for organizations. Focus should be placed on the most critical areas of identity risk first.

1 Enterprises can start by shedding their dependency on passwords, especially for privileged accounts, remote access and high-value applications and systems. Use phishing-resistant methods that do not fall back to a password.

2 Incorporate deterministic identity security controls. Probabilistic security methods operate on the basis of likelihood of risk, introducing gaps that attackers can exploit (and can do so even faster and more effectively with AI). By contrast, deterministic controls provide binary certainty if something is true or false, safe or a threat, and allow or deny an action based on that surety. Phishing-resistant MFA is deterministic, passwords are not.

3 Make sure that the credentials used to access systems are always linked to a legitimate, verified person. This means instituting processes to re-verify identities with high levels of assurance at high-risk moments, such as resetting account access.

4 Implement identity-specific risk detection and mitigation strategies that leverage, using a wide spectrum of risk signals. This includes risk data being collected by other security tools, such as endpoint-deployed solutions for detection and response.

Equally important to implementing the right technology is working with a partner well-versed and ready to support the change management required.

HYPR's Passwordless Identity Assurance stops modern identity attacks while removing friction from identity processes. With HYPR, you can detect, prevent, and eliminate identity-related risks at every point in the identity lifecycle, ensuring your workforce are who they claim to be at all times. Designed to integrate rapidly into existing infrastructure, HYPR is deployed at scale in organizations across the globe for both employee and customer scenarios.

Appendix: Scope and Methodology

HYPR commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 750 IT security DM respondents were interviewed in February and March 2024. Respondents were targeted in the US (250), UK (165), France (105), Germany (105), China (45), Australia (40) and Japan (40), and were from organizations with 50+ employees across a range of private and public sectors.

Interviews were conducted online using a rigorous multi-level screening process to ensure that only suitable candidates were given the opportunity to participate. Unless otherwise indicated the results discussed are based on the total sample. Additionally, HYPR researchers analyzed anonymized endpoint event data collected through the HYPR platform.

Sources

1. https://www.evanta.com/resources/ciso/blog/8-trends-for-cisos-in-2024
2. https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-057a
3. https://www.darkreading.com/cloud-security/mfa-bombing-attacks-target-apple-iphone-users
4. Based on an analysis of user data, login information and device risk collected by HYPR over a 90-day period.
5. Based on an analysis of user data, login information and device risk collected by HYPR over a two week period.

VansonBourne

About Vanson Bourne:

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision makers across technical and business functions, in all business sectors and all major markets. For more information, visit **www.vansonbourne.com**

HYPR

About HYPR:

HYPR creates trust in the identity lifecycle. HYPR Identity Assurance provides the strongest end-to-end identity security for your workforce and customers, combining phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. With an independently validated ROI of 324%, HYPR secures some of the most complex and demanding organizations globally, including 2 of the 4 largest US banks, manufacturers and leading critical infrastructure companies. For more information, visit **www.hypr.com**

See how HYPR helps secure your workforce and customers
Visit: hypr.com/get-a-demo