THE STATE OF AUTHENTICATION IN THE FINANCE INDUSTRY

2022

VansonBourne | HYPR

Contents

Foreword

Cybersecurity continues to be both a strategic priority and one of the biggest challenges for every organization — regardless of size, sector, budget, or geographic location. As the attack landscape is ever changing, we need to evolve our strategies to stay current. For IT leaders do that, we need to recognize that certain attack vectors remain the perennial cause of an outsized number of breaches.

The finance industry has frequently been at the forefront of cybersecurity both because the sector is one of the most targeted, but also because the companies in the sector are among the most likely to adopt new defensive technologies. While organizations invest heavily in security measures at the perimeter, inside the network, and through behavioral analytics, authentication security has not moved at the same pace.

As accountable leaders, we strive to protect our organizations from cyberattack, but the headlines and the findings of this report explicitly demonstrate that there is more to do in the space of authentication security. While we're focused on the radical changes in the threat landscape, we must recognize the fact that most breaches are directly attributable to gaps in the security around authentication.

This report shines an important spotlight on the perceptions of global financial institutions around authentication. As the study findings show, there remains much to do to close these security gaps, and traditional MFA methods are not delivering the security that we all need.

The impact of these risks extends beyond the breach costs quantified in this report. Business disruption costs, customer impact or even loss, reputation damage, all can have a material and lasting impact on an organization.

So, what needs to change? As a former CIO and CTO within financial services, I've seen the evolution and increasing sophistication (one might even say professionalism) of the attackers and the ways that they target the industry. We are at a tipping point for change — it is time to adopt more contemporary authentication and access methods in the same way we have tackled other elements of security. Allowing username and password – even if supplemented with some form of MFA – to be the gatekeeper into our systems and data represents a risk we can now mitigate. Adopting truly secure and phishing-resistant passwordless multi-factor authentication practices and technology can afford the contemporary protection that we need.

— David Reilly

Cyber Security and Financial Services Strategic Advisor

Formerly, CIO and CTO for Bank of America, CIO at Morgan Stanley, Technology Infrastructure, CTO at Credit Suisse and Managing Director of Global Technology Operations at Goldman Sachs.

Introduction

Under modern business models, financial service organizations, of any size, must be able to efficiently and securely access a wide variety of digital resources. This places an enormous strain on their IT and security teams to ensure operations run smoothly and cybersecurity defenses are kept up to date and airtight.

Financial organizations rely on authentication security to make sure that the right people can access the right systems and data — and to keep others out. As the most highly targeted industry for cyberattacks, it is fair to say that financial organizations are at the forefront in adopting security innovations. Yet, despite being trailblazers, we consistently hear about new, stealthy and more advanced techniques that can circumvent common authentication protocols and infiltrate financial systems. For a sector under the watchful eye of regulators, and other industries taking note, the question remains — how do their authentication methods and technology stack up against looming threats?

Additionally, for an industry where friction and obstacles to access can have an outsize impact on the bottom line, financial institutions are focused more than ever on balancing security and user experience – two aspects that haven't always gone hand-in-hand. So, how are authentication trends affecting user experience and other areas critical to a leading-edge business? Where do financial organizations stand when it comes to newer authentication technologies such as passwordless authentication?

In order to determine the current state of authentication security in the finance industry, we interviewed 500 IT decision makers with knowledge and responsibility for cybersecurity in the financial services sector. These IT security decision makers were from organizations in the US and Europe, ranging in size from 50 employees to large enterprises. This report presents the results, exploring several areas including the following:

- → **Cyberthreats and their impact on financial services organizations**
- → **Current authentication practices and shortcomings**
- → **Perceptions and misconceptions about authentication security**
- → **The impact of passwordless authentication**

Key Findings

3.4

breaches reported annually by financial services organizations, on average

80%

of financial services organizations have experienced a breach that was likely related to authentication weaknesses

$2.19M

average cost of authentication-related cyber breaches annually

90%

consider their organization's authentication approach to be secure, yet widespread use of insecure methods is prevalent

89%

believe that passwordless authentication is needed to ensure user satisfaction

89%

state that passwordless authentication ensures the highest level of authentication security

90%

agree that passwordless authentication has cost benefits over traditional authentication methods

1

Financial Services Authentication Is Failing, Resulting in Multiple Attacks and Breaches

Financial Organizations Face Continuous, Evolving Cyber Threats

Financial service organizations continue to be targeted by cyberattacks. Nearly all (94%) surveyed financial service organizations faced some type of attack over the past 12 months, with phishing (36%) remaining the most prevalent.

The threat from push notification attacks is also significant (29%), particularly among organizations in the US (38%). Sometimes called MFA-prompt bombing, push attacks specifically target the push notifications used by many authenticators. It is a favorite technique of modern hacking groups, including Lapsus$, which recently breached Okta, Microsoft, Samsung and others.

With new threats constantly emerging, organizations must secure themselves against known attacks while making sure they are able to address future attack methods. Approaching this proactively is paramount, and the right authentication methods are a key part of that process.

Types of Cyberattacks Faced in the Last 12 Months

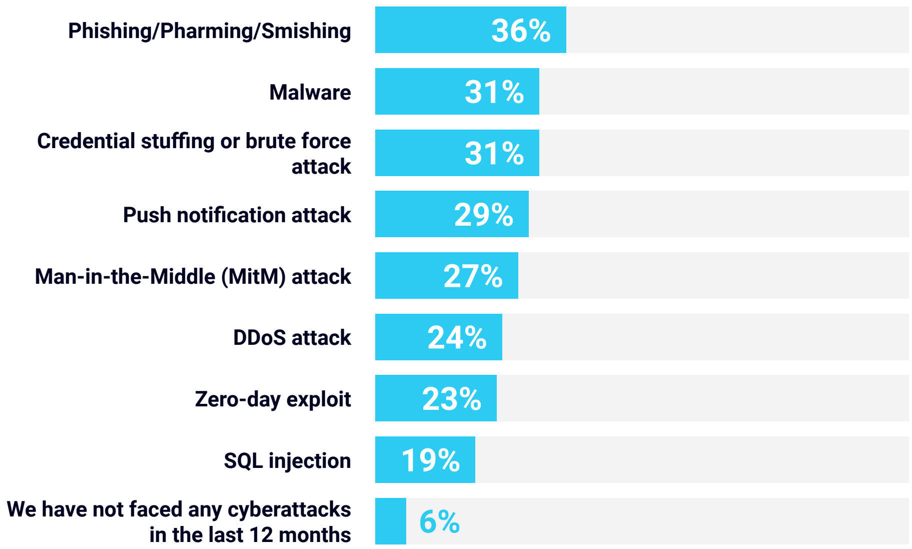
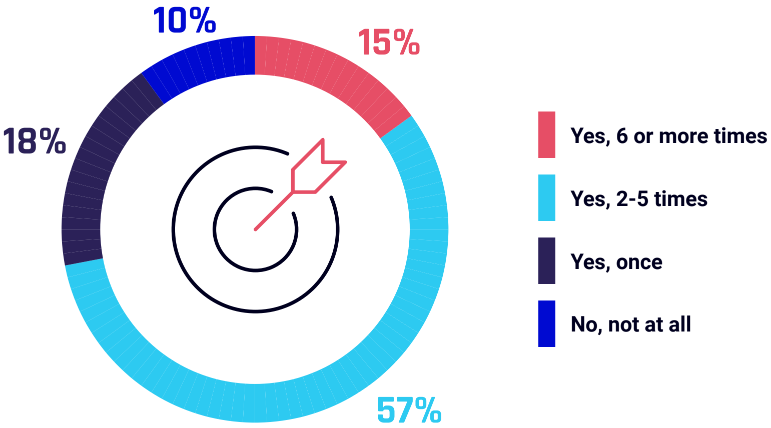


Figure 1: What, if any, types of cyber-attack has your organization faced in the last 12 months? [500], omitting some answer options

These Cyberattacks Frequently Result in Successful Breaches

Despite a stated confidence in their authentication security measures (see Section 3), they aren't enough to prevent attacks from breaching organizations. Of the financial companies that reported an attack, 90% acknowledge that they fell victim to a cyber breach over the past 12 months. Put differently, 85% of all financial services organizations experienced a known breach. Moreover, nearly three quarters (72%) who experienced a breach did so multiple times — at an average of 3.4 breaches. This not only demonstrates the prevalence of attacks, it exposes the vulnerability of current security measures in place and the damage caused by reluctance or inability to make tangible changes.

Did Your Organization Experience a Cyber Breach in the Last 12 Months?



3.4
faced on average

Figure 2: Was your organization the victim of a cyber-breach as a result of any cyber-attacks in the last 12 months? Only asked to respondents whose organization has experienced a cyber-attack in the past 12 months [468], omitting some answer options

The Root of It All? Authentication Vulnerabilities

Digging into a specific cause of breaches, 95% of organizations that were breached admit that credential misuse or authentication vulnerabilities were presumed to be a factor. This translates into the astounding fact that **80% of all financial services organizations experienced at least one cyber breach related to a weakness in authentication.**

When looking at different segments and geographies, we find some interesting trends. 75% of large banks (500+ employees) and 90% of smaller banks (50-499 employees) have all experienced a breach that they believe to be authentication related. On a regional basis we see that UK organizations report the fewest cyberattacks of any geography (82% vs. an average of 94%), plus those attacks are less likely to lead to a breach (80% vs. an average of 90%). A reflection of the UK's strict regulatory stance? Perhaps, but it's not enough when it comes to authentication security as those breaches that do occur are attributed to authentication vulnerabilities at the same rate as other countries.

These findings highlight a serious flaw in how many financial service organizations are protecting themselves, and shows why they need to take a harder look at their current authentication protocols.

Cyber Breaches Related to Credential Misuse or Authentication Vulnerabilities

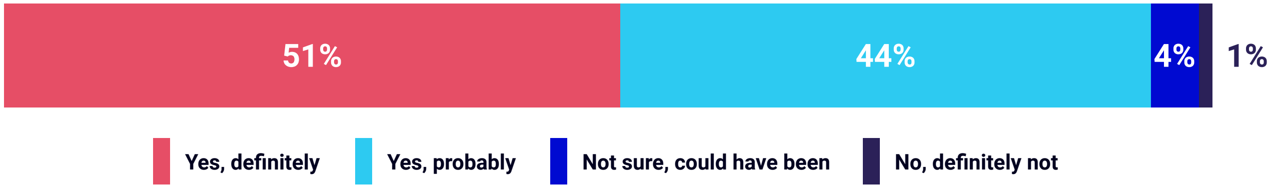


Figure 3: Were any of the cyber-breaches that your organization experienced related to credential misuse or authentication vulnerabilities? Only asked to respondents whose organizations have been the victim of a cyber-breach as a result of a cyber attack in the past 12 months [423]

What About Ransomware?

34%

of financial services organizations surveyed were hit by ransomware attacks in the past 12 months.

With authentication weaknesses attributed to successful attacks on 80% of organizations, strong authentication should be a part of any ransomware defense.

There's a Massive Financial Impact From Cyber Breaches Related to Authentication

Organizations who have experienced an authentication-related breach estimate a staggering average cost of $2.19 million (in the last 12 months).

Moreover, that figure is presumably based on direct cost factors, such as fines, ransom fees, customer notifications and immediate loss of business. There are many intangible and hidden costs, such as long-term remediation work, operational disruption, reputation damage, and cyber insurance premium increases that can increase that by orders of magnitude.

As you'd expect, larger businesses face higher costs — $2.8 million, on average vs. $1.6 million for small organizations. And by country, those in the US report the greatest cost across all business sizes ($3.1 million); a much larger sum than those in France ($1.4 million), Germany ($1.6 million) and the UK ($1.7 million).

$2.19M

average cost of authentication-related cyber breaches annually

Despite the Financial and Business Consequences, Most Organizations Didn't Change Their Authentication Methods

Almost all (99.5%) organizations who suffered a successful cyber breach felt an impact off the back of it. Nearly one-third lost customers to their competitors. Other major consequences included regulatory fines, theft of employee data, and theft of customer data.

A few organizations are learning from their mistakes. More than one-third (37%) made changes to their authentication methods following a breach. But this means that **63% did nothing to improve their authentication protocols.** In other words, nearly two-thirds of these financial service organizations are still highly exposed to future attacks and breaches, with all the accompanying financial and business fallout.

Impact of Cyber Breaches Experienced Over the Last 12 Months

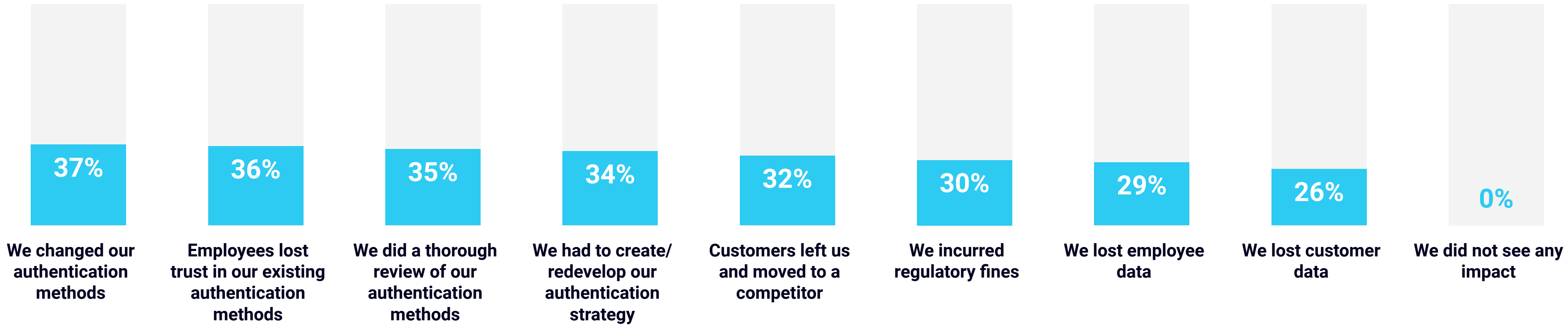
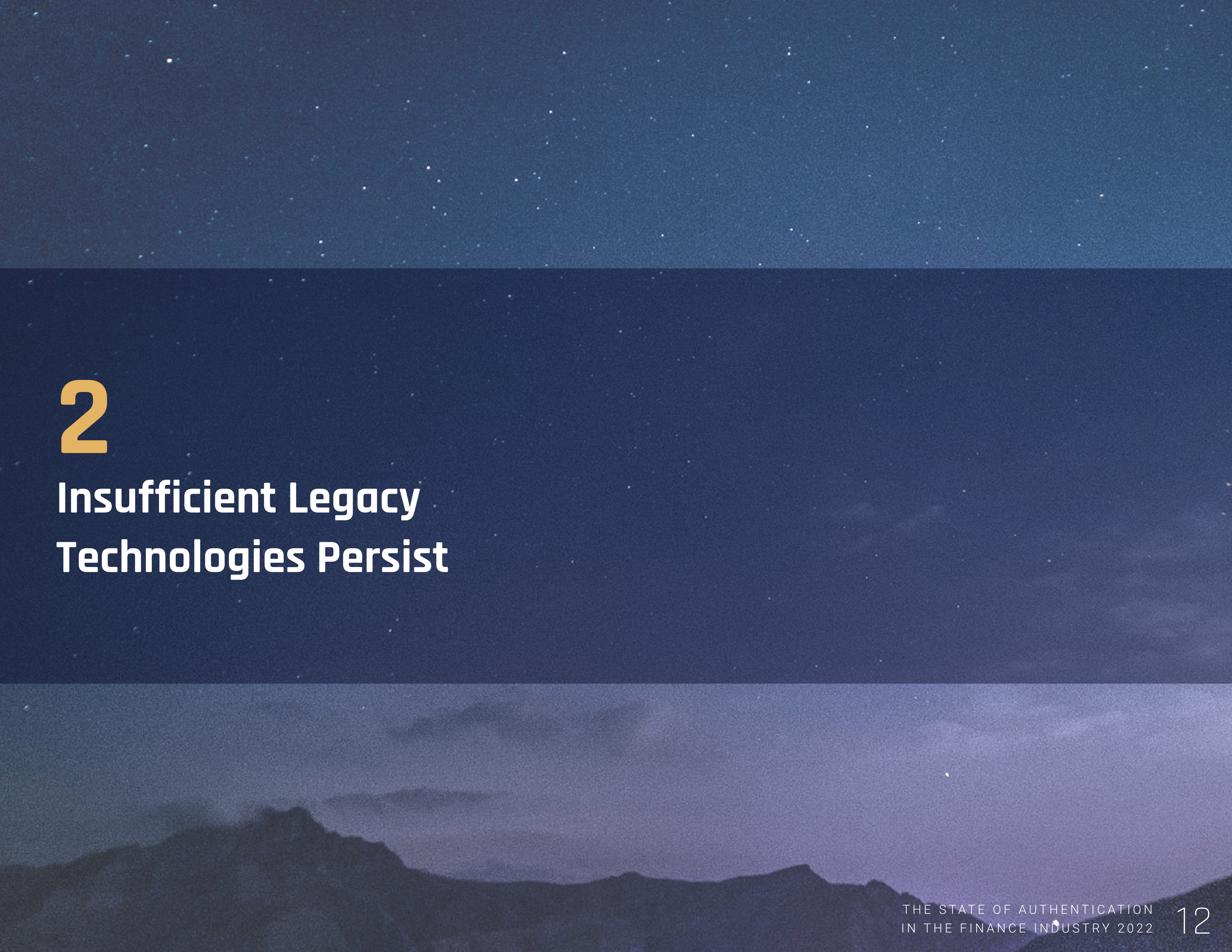


Figure 4: What was the impact of the cyber-breach(es) that your organization experienced in the last 12 months? Only asked to respondents whose organizations have been the victim of a cyber-breach as a result of a cyber attack in the past 12 months [423], omitting some answer options



2

Insufficient Legacy Technologies Persist

Insecure Methods of Authentication Are Still Widely in Use

Customer Authentication Practices Even Less Secure

While this report primarily focuses on workforce authentication, we took a quick pulse on the customer-side and found insecure practices to be even more prevalent, with 43% of financial services organizations using traditional MFA methods for customer authentication, 38% using social identity credentials, and 28% requiring only username and password.

A few years ago, multi-factor authentication (MFA) would have been the de-facto cybersecurity recommendation for businesses. But while traditional MFA methods were once considered best practice, increasingly sophisticated attackers have worked to circumvent it, making it much less effective as a defense measure. This has prompted calls by various regulatory bodies, including the United States Cybersecurity and Infrastructure Security Agency (CISA), for the use of MFA that can resist phishing and other attack methods.

Yet, awareness of this is either sparse or ignored among surveyed IT security decision makers in financial service organizations. Instead, substantial proportions report that their employees use legacy technologies such as SMS and OTPs, and incredibly, around a quarter (22%) are using usernames and passwords only for authentication. This leaves organizations highly vulnerable to modern cyberthreats, particularly in a remote and distributed working world.

Workforce Authentication Methods in Current Use

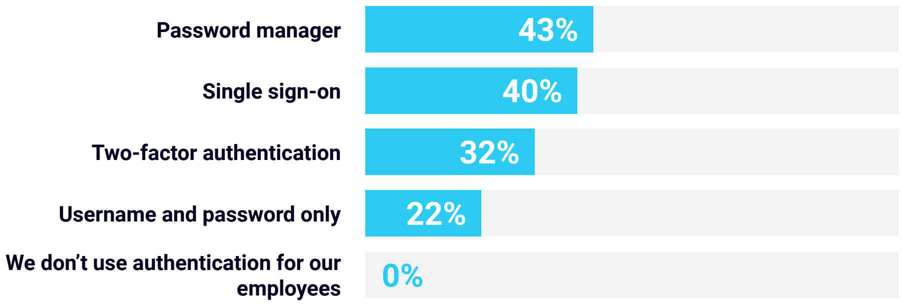


Figure 5: Which of the following authentication methods does your organization currently use for its employees? [500], omitting some answer options

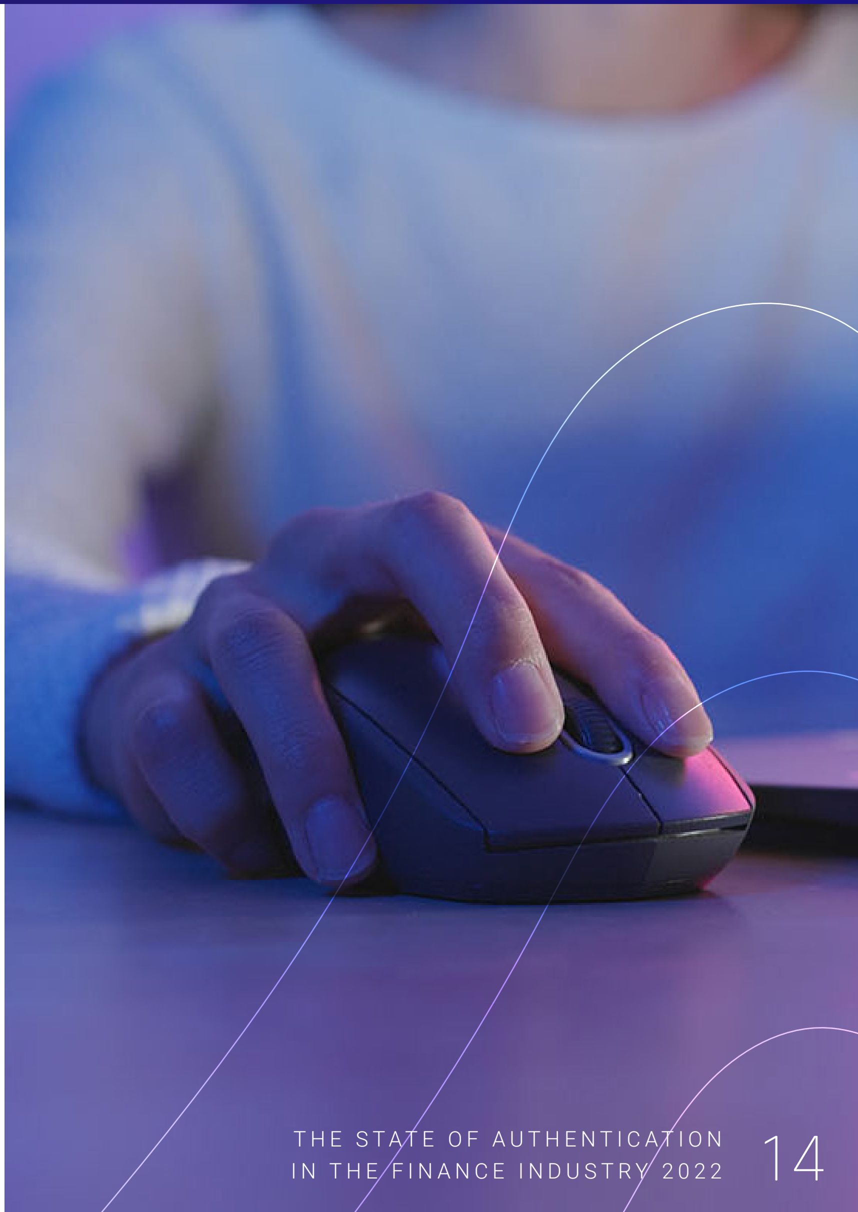
Despite Belief in the Importance of Desktop Authentication, Current Authentication Methods Do Not Support It

Another distinct flaw in the authentication methods currently in use is that most sit at the application level. For best protection, authentication must be performed at the OS/desktop/workstation level, as agreed by 90% of respondents. But they are not practicing what they are preaching, with many using methods that do not support desktop-level authentication.

From the desktop, an attacker can often access valuable resources and directly connected apps and services. Users frequently store confidential data or files on the local drive. Passwords for a variety of applications and sites may be stored locally or cached in the browser. Organizations reassess their authentication security across the board, starting with the very first login to the endpoint, in order to harden their defenses against modern cyberthreats.

90%

agree that for best protection, authentication must be performed at the OS/desktop/workstation level



Most Organizations Need Significant Authentication Improvements

Pain Points Faced With Authentication Methods

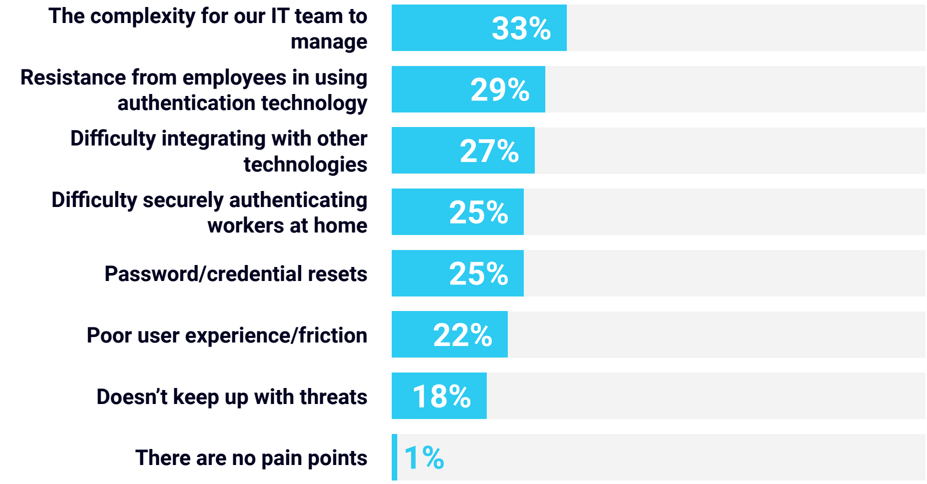


Figure 6: What are the pain points associated with your organization's authentication methods? [500], omitting some answer options

There's near unanimous agreement (99%) that current authentication methods are not cutting it. Financial services organizations are experiencing a variety of pain points with their existing technology, specifically when it comes to user experience, IT experience and security.

Three-quarters (75%) of organizations face IT-related obstacles, including management complexity (33%) and integration difficulties (27%). 62% state their authentication methods cause difficulties for users, often leading to resistance in adoption from employees (29%). A similar proportion (57%) name security issues, with difficulty securely authenticating remote employees a particular concern (25%).

Current authentication practices are leaving financial organizations with authentication challenges and cracks in their security. Yet, as we'll see, there seems to be a (willful?) blindness about how wide these gaps really are.

Pain Points Are Impacting Multiple Areas:

75%
IT-related

62%
UX related

57%
security related

3

Authentication Security Misconceptions Are Thwarting Progress

Despite the Insecure Methods in Use, Organizations Believe Their Authentication Approach Is Secure

There is a broad confidence in the security of organizations' approaches to authentication, with nine in ten saying that their approach is mostly or completely secure. Yet, this faith is dangerously misplaced given that 80% of organizations were breached in the last 12 months due to believed authentication vulnerabilities.

The breaches are hardly surprising given the insecure authentication methods organizations are using. What does surprise us is the seeming disconnect between perceived and actual authentication security. Especially with the recent high-profile attacks stemming from authentication weaknesses, such as the Colonial Pipeline ransomware attack that forced the shutdown of the largest pipeline in the U.S. Or the $24 million stolen this year from the cryptocurrency exchange Crypto.com after hackers found a way to bypass their MFA controls.

Perceptions on Organizations' Level of Authentication Security

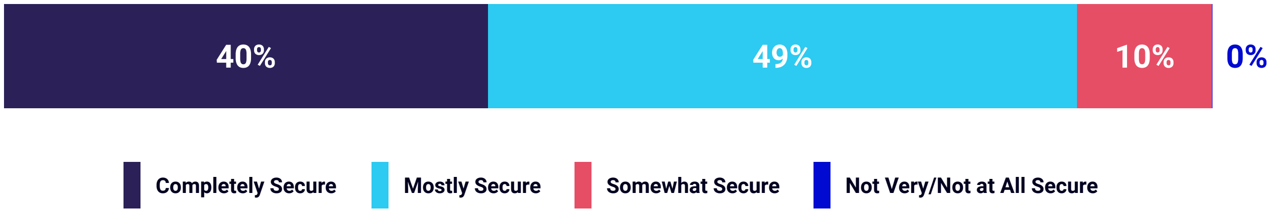
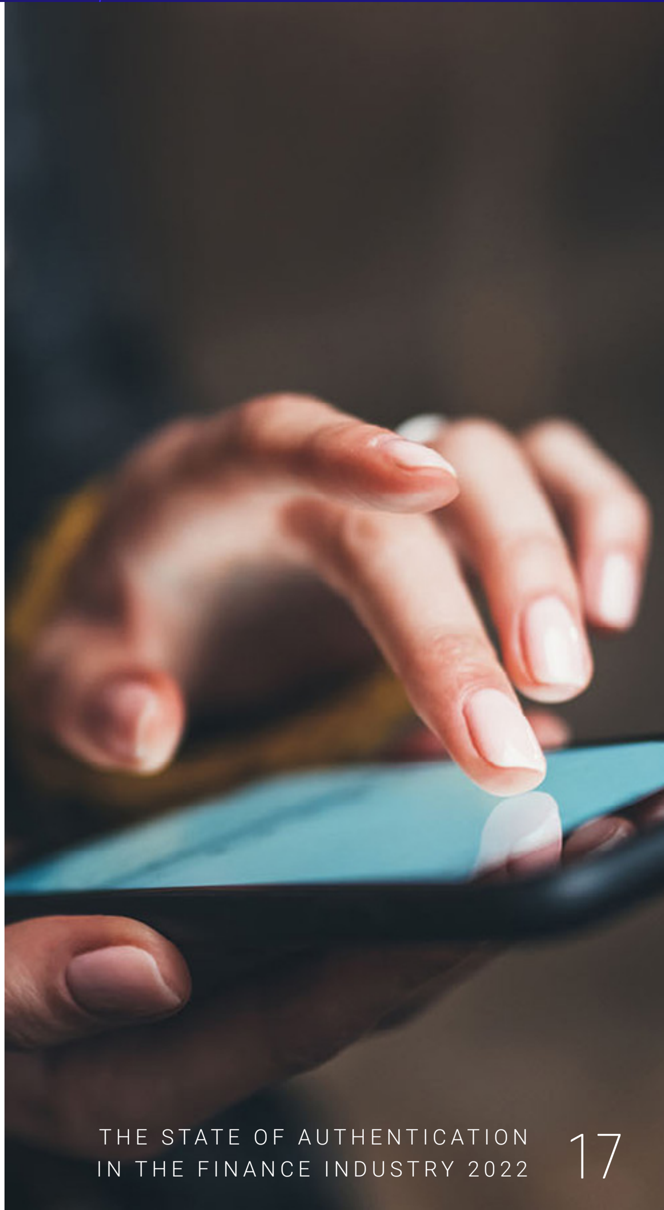


Figure 7: How secure do you consider your organization's approach to authentication to be? [500], omitting some answer options



There's an Overconfidence in Traditional MFA

The disconnect between perceived and actual levels of authentication security makes more sense when we see respondents' attitudes toward traditional MFA. The vast majority (84%) feel that traditional MFA provides complete security. But this confidence is misguided. While better than just a username and password, these legacy MFA methods are struggling in an ever-evolving cyberthreat landscape.

Attackers use automated toolkits, sophisticated social engineering tricks and other attack techniques to bypass the MFA controls that financial services organizations put in place. Yet, despite facing attacks on their MFA processes, including the 29% hit by push attacks, this message clearly hasn't sunk in.

84%

feel that traditional MFA provides complete security

We See the Same Misconceptions When It Comes to Phishing-Resistant Authentication

Many organizations are using legacy authentication methods which can be easily phished. Yet over nine in ten (92%) respondents state that phishing-resistant multi-factor authentication should be used by all organizations.

Even more startling, nearly half (47%) believe that phishing-resistant multi-factor authentication already is key to their authentication strategy and another 51% believe it plays a part. There is obvious confusion here, highlighting a need for better education and training around which authentication methods are and aren't phishable.

It also further suggests that organizations are not as secure as they think that they are, and that their current authentication methods need attention.

4

Passwordless MFA Is the Way Forward

Misperceptions About Passwordless Authentication Make Organizations Vulnerable

Use of Passwordless Authentication in Organizations

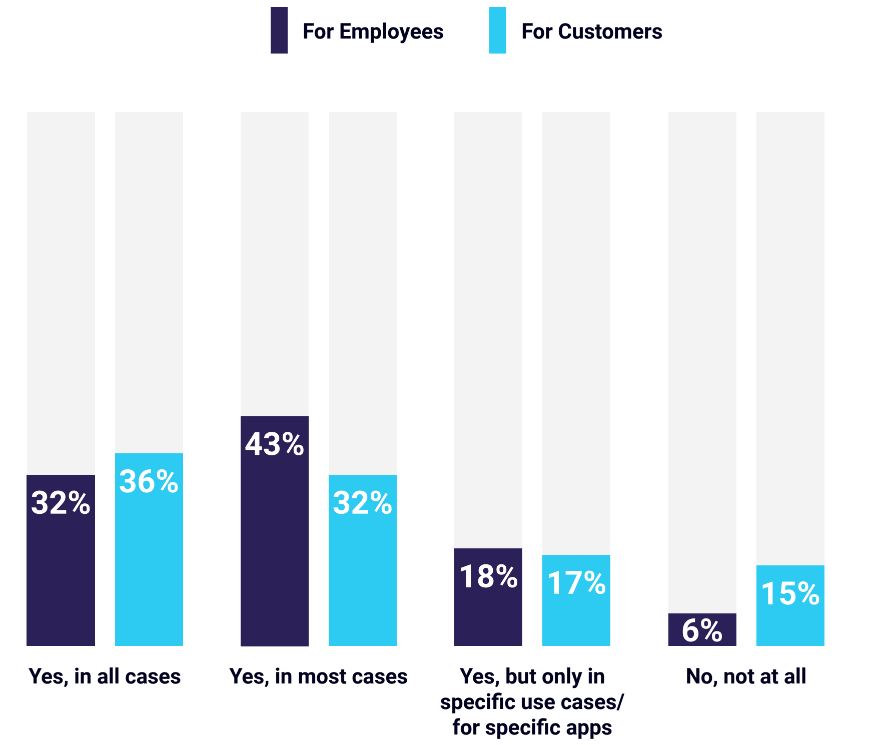


Figure 9: Does your organization use passwordless authentication today? [500], omitting some answer options

True passwordless MFA eliminates the need for passwords and shared secrets across the business, enabling more secure working, particularly in the remote world we now live in. It's the gold standard for authentication, and many respondents believe that their organization already Is using it.

However, in actuality, many organizations are still using authentication methods that require passwords at some stage, such as password managers, legacy MFA, and single sign-on. As we saw with responses about traditional vs. phishing-resistant MFA, there is clearly a misconception of what constitutes real passwordless multi-factor authentication. This lack of knowledge heightens the false sense of security that is contributing to breaches of financial organizations.

Passwords Are Still Causing Finance Organizations Pain; Passwordless Authentication Offers the Cure

We all know the pitfalls and frustrations of passwords, which are echoed by IT professionals in financial service organizations. The requirement for complex (hard to remember!) passwords (37%), the frequency of resetting them (36%), and sheer number of different passwords required to perform one's job (35%) are all stated pain points. It's therefore unsurprising that respondents name improving the user experience (34%) as one of the main benefits to passwordless authentication.

Moreover, it's not just end users affected by those issues. Our survey found that, on average, 15% of organizations' annual help desk budget goes to password-based authentication issues and resets. This expense could be saved by using passwordless authentication. And that's before factoring in the associated costs, such as lost productivity.

The next most common benefits expected from a passwordless experience are increasing cybersecurity (33%), meeting cyber insurance requirements (31%) and improving supply chain security (31%) — an often neglected, but critical area to protect.

Benefits to Passwordless

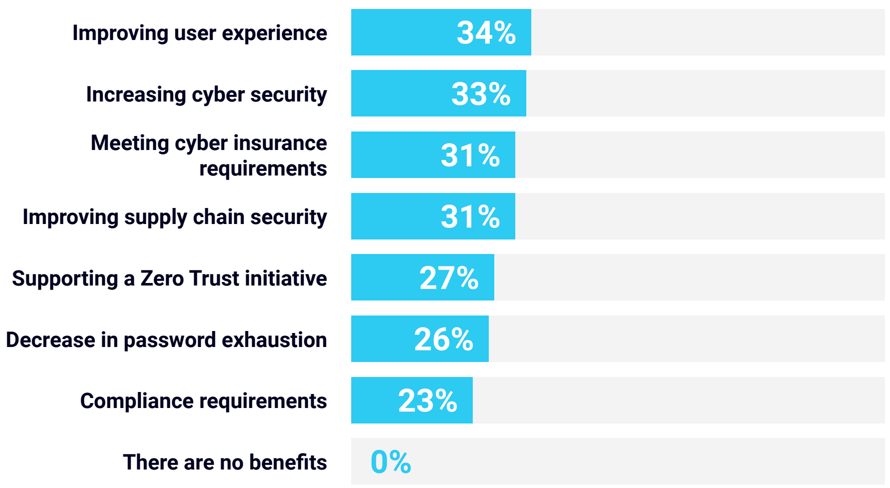


Figure 10: In general, what are the benefits to organizations using passwordless authentication methods? [500], omitting some answer options

Organizations Are Ready for Passwordless Authentication

Three key focuses of any IT team are security, usability and of course, value for money. Authentication-related breaches cost financial organizations $2.19 million each year, on average. The authentication methods used today add friction to the login process and don't deliver the required security. For many right now, authentication isn't ticking any of their boxes.

Respondents to our survey recognize that passwordless MFA fixes their authentication shortcomings by positively impacting security, user experience and the bottom line.

90%

agree that passwordless authentication has **cost benefits** over traditional authentication methods

89%

state that passwordless authentication provides the **highest level of authentication security**

89%

report that organizations need to fully embrace passwordless authentication to **ensure user satisfaction**

Conclusion

As the financial industry continues to transform and modernize its operations and business models, organizations face unprecedented and dynamic security risks. Rapid digitization, interconnection with third-party systems, migration to the cloud, and shifts in working patterns, all open new attack vectors for which cybercriminals are quick to take advantage. The biggest area of vulnerability remains the credentials and authentication protocols that protect the point of access to these systems.

Most organizations' authentication approaches are failing to keep up with current threats, yet alone those more sophisticated on the horizon, resulting in breaches that cost $2.2 million dollars a year. On top of that, their approaches are adding friction and frustration for users and IT teams alike.

Based on the findings, security and IT leaders are aware of the tools and actions for success, yet the financial services industry is clearly missing the mark. So why are financial services organizations still sticking with the same technology when they admit there's a better way?

The time for passwordless is now

Financial services organizations need to take up their mantle as security innovators and fully embrace phishing-resistant passwordless authentication technology.

HYPR True Passwordless™ MFA delivers the security assurance and frictionless experience financial services organizations require, with phishing-resistant login that begins at the desktop and extends to the cloud. Designed to deploy rapidly into existing infrastructure, it turns an ordinary smartphone or other device into a PKI-backed security key. HYPR is deployed and battle-tested in some of the largest banking and financial institutions in the world — 3 of the top 4 banks are HYPR customers.

Research Scope/Methodology:

HYPR commissioned independent technology market research specialist Vanson Bourne to undertake the quantitative research upon which this whitepaper is based. A total of 500 IT security DM respondents, equally split between organizations with 50-500 and 500+ employees, were interviewed in April and May 2022. Respondents were targeted in the US (200), UK (100), France (100) and Germany (100). All respondents were from organizations in the financial services sector, including financial institutions (banks) digital banking and FinTech, investment (retail), wealth management, insurance, investment (commercial) and capital markets.

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.

VansonBourne

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.

Learn more at www.vansonbourne.com

HYPR | *THE PASSWORDLESS COMPANY*

HYPR fixes the way the world logs in. HYPR's true passwordless multi-factor authentication (PMFA) platform eliminates the traditional trade-off between uncompromising assurance and a consumer-grade experience so that organizations decrease risk, improve user experience and lower operational costs.

To see how passwordless MFA can secure your financial services organization
Visit: hypr.com/demo