datos INSIGHTS

July 2024

Next-Generation MFA: Security Assurance for the Modern Enterprise

John Horn

This report provided compliments of:

Token

July 2024

Next-Generation MFA: Security Assurance for the Modern Enterprise

John Horn

datos INSIGHTS

Table of Contents

List of Figures

Summary and Key Findings

Multifactor authentication (MFA) has existed for more than 20 years and is well-known across industries and society. Financial services (FS) CISOs have deployed MFA to defend their digital enterprises against cyberattacks and resulting business risk. Enterprise workforce users (e.g., employees, contractors, consultants, business partners) leverage various MFA solutions to gain access to the digital enterprise to leverage or contribute to enterprise services.

Traditional MFA is woefully inadequate to defend against today's threat vectors targeting FS corporate enterprises. This is not new news. Traditional MFA has been defined as users demonstrating their identity through authentication factors of *multiple* categories (e.g., something known by the user, something possessed by the user, something inherent to the user).[1] In practice, traditional MFA presumes the use of a *password* as one of these knowledge factors. However, over the past decade, passwords and other knowledge-based factors have become easily compromised through thousands of data breaches, effective account takeover and phishing schemes, and poorly created passwords.

In response, market providers developed improved solutions called phishing-resistant MFA (also known as passkeys or certificate-based MFA) based on the FIDO2 industry standard. These solutions deliver higher security *assurance* (stronger confidence) and *resiliency* (ability to function properly while under attack). Datos Insights advised financial institutions and insurers of the need to migrate to phishing-resistant MFA in September 2022. The U.S. federal Cybersecurity and Infrastructure Security Agency (CISA) strongly urged phishing-resistant MFA in October 2022.

In 2024, while cybersecurity attacks against enterprises continue to advance, the adoption of phishing-resistant MFA within FS remains slow. As the costs of data breaches and ransomware attacks continue to escalate, financial institutions, insurers, and other FS firms must ask these essential business questions: What kinds of MFA options deliver even higher security assurance and resiliency for the business while improving user experiences? Where do we go beyond phishing-resistant MFA for our most business-sensitive enterprise functions?

---

[1] "Glossary, MFA," National Institute of Standards and Technology Computer Security Resource Center, accessed July 1, 2024, https://csrc.nist.gov/glossary/term/mfa.

The term next-generation MFA (NG MFA) has emerged to classify these higher-order solutions. An NG MFA solution based on smart ring technology was recently introduced to the market. The solution qualifies as phishing-resistant MFA, with no passwords or knowledge-based factors that the user could forfeit to an attacker. Datos Insights conducted a study of North American CISOs to understand important practical considerations regarding this wearable solution and its deployment within FS. This report describes the research and includes analysis and recommendations to CISOs to optimize the solution's value for the business. Key findings for this report follow:

- **Phishing attacks against workforce users, supply chain attacks from third parties, and ransomware attacks were identified as the top enterprise cyber risks for the CISO.** Each attack vector is advancing in sophistication through criminals using artificial intelligence (AI) capabilities, making them more difficult for CISOs and their teams to defend against. As phishing is so prevalent in current markets and a major component of these cyber risks, the solution mitigates these top risks. With high cyber risk threatening FS, this single solution, deployed correctly, significantly improves the risk calculus for the business.

- **CISOs most need to improve risk management for system administrators despite having privileged access management (PAM) solutions.** PAM solutions have functioned as the historical norm for CISOs managing system admin risks. Still, with the rise of phishing and insider attacks, CISOs map NG MFA deployment foremost against this important business risk.

- **Senior executives at many FS firms lack robust security solutions aligned with their functions and business risk.** Almost none of the CISOs interviewed had distinct controls deployed for their executive users. With spear-phishing and other techniques on the rise, this gap was somewhat concerning.

- **Fifty-nine percent (59%) of CISOs expressed high interest in considering NG MFA wearable form factor for their workforce.** After understanding how the solution functioned, many CISOs recognized the stronger security assurance, mapped the solution against known high-risk areas for specific portions of the workforce, and requested a solution deep dive to scope a proof-of-concept deployment at their firm.

- **Security, ease of use, and recovery from lost rings were the top capabilities most desired by CISOs.** Cost is always important, but CISOs ranked cost eighth out of the nine value drivers for the solution.

- **Most CISOs view introducing NG MFA wearables as a major cultural change for the organization.** They are correct. Planning and training for workforce introduction is a critical component for success.
- **The CISO is the budget holder for 94% of FS firms interviewed.** Given the lack of familiarity with wearables in most organizations, CISOs will likely consult with several peers during the procurement process and collaborate during deployment planning.

Introduction

In the modern age, cybercriminals defeat passwords and antiquated MFA mechanisms with ease. In 2023, cyberattacks resulted in 2,365 breaches worldwide, impacting an estimated 343,338,964 victims.[2] The Better Identity Coalition estimated that 80% of these breaches were related to stolen, weak, or reused passwords.[3] CISA reports that phishing attacks account for 90% of ransomware attacks.[4]

As these attacks have increased, the workforce has dispersed. Of the many unprecedented aspects of the recent COVID-19 pandemic, employees working from home became the norm. With cyberattacks advancing rapidly, CISOs were suddenly thrust into urgent work of modernizing and securing the expanded corporate enterprise.

The traditional means for avoiding phishing attacks relies on training users to identify phishing attacks. As cybercriminals increasingly use AI capabilities within phishing attacks, the effectiveness of users to self-identify these attacks is ending. FS firms require a new class of tools called phishing-resistant MFA solutions (also known as passkeys), the modern MFA standard for FS firms.

Biometrics and wearable technology have also emerged in the market. Consumers can scarcely operate today without their mobile device (with its embedded biometric capabilities) in close proximity. Wearables such as the Apple Watch have also become mainstream. Smart rings have emerged as the next big wearable. Smart rings track everything a smartwatch does (such as sleep, activity, and wellness) with a more discreet form factor and longer battery life. Smart rings offer premier levels of security assurance by assessing hundreds of biometric points on the user's chosen finger (Figure 1).

---

2 "Policy Forum: Identity, Authentication and the Road Ahead," Better Identity Coalition, FIDO Alliance, and the Identity Theft Resource Center, January 25, 2023.

3 "Better Identity Coalition: Better Identity at Five Years: An Updated Blueprint for Policymakers," Better Identity Coalition, January 2024, accessed February 28, 2024, https://static1.squarespace.com/static/5a7b7a8490bade8a77c07789/t/65b00995dd1af8633cbce40c/1706035608068/Better_Identity_Coalition24.pdf.

4 "Stop Ransomware," CISA, accessed July 3, 2024, https://www.cisa.gov/stopransomware/general-information.

Figure 1: Smart Ring

Source: Token

CISOs may now consider how smart ring biometric capabilities can reduce cyber risk for their business. The objectives of this research study were to understand FS CISO appetite and considerations for how NG MFA solutions would be used within the enterprise workforce for sensitive business functions, especially when mapped against top cyber risks for the business. The findings and recommendations from this research inform both the security and practical culture of the modern FS digital workforce.

Methodology

This research study, commissioned by Token, sought the insights and perspectives of 18 FS CISOs and workforce MFA leaders across the U.S. Eight CISOs served FIs, six served insurers, three served digital banking processors, and one served a top-three investment advisor. Datos Insights used an interview guide within qualitative 60-minute video interviews to examine CISO perspectives in depth. The research focuses on enterprise (corporate) risks and solutions, not customer-facing services.

Enterprise Cyber Risk Perspectives

As workforce MFA owners, CISO assessments of cyber risk drive the prioritization of security resources and funding. The study sought to understand CISO perspectives for existing cyber risk as well as improvement opportunities.

Top Cyber Risks to the Enterprise

CISOs were asked to identify (in order) the top three cyber risks to their enterprises, i.e., the vectors that generate the most difficult business risks. A point system was used to tabulate responses. **Figure 2** summarizes the results.

Figure 2: Top Cyber Risks for the FS Enterprise

Points awarded by priority level
Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

The key findings follow:

- **Phishing attacks against the workforce ranked as the highest cyber risk category.** Criminal teams have become increasingly effective at running phishing campaigns against different teams within the workforce, harnessing the power of AI, especially for organizations that have not implemented phishing-resistant MFA. Most FS institutions

have implemented some kind of MFA. However, organizations that rely on traditional, knowledge-based MFA have become the most vulnerable, easy prey for criminal teams. Others deploying MFA based on one-time passcodes or push notifications have also fallen on difficult times as cybercriminals defeat these mechanisms routinely. The slowness of FS institutions to deploy phishing-resistant MFA has extended the effective lifetime for these attack vectors. Some CISOs were most concerned about system admin resources and their vulnerability to phishing attacks. These entrusted individuals hold a premium level of data access and perhaps the highest degrees of business risk. Other CISOs were more concerned about phishing attacks against junior-level employees—roles with higher turnover rates—who may be more trusting and vulnerable to attacks, such as call center employees. DevOps leaders also hold risk, as do executives within the organization. For many FS institutions, phishing against the enterprise workforce is the top cyber risk in 2024.

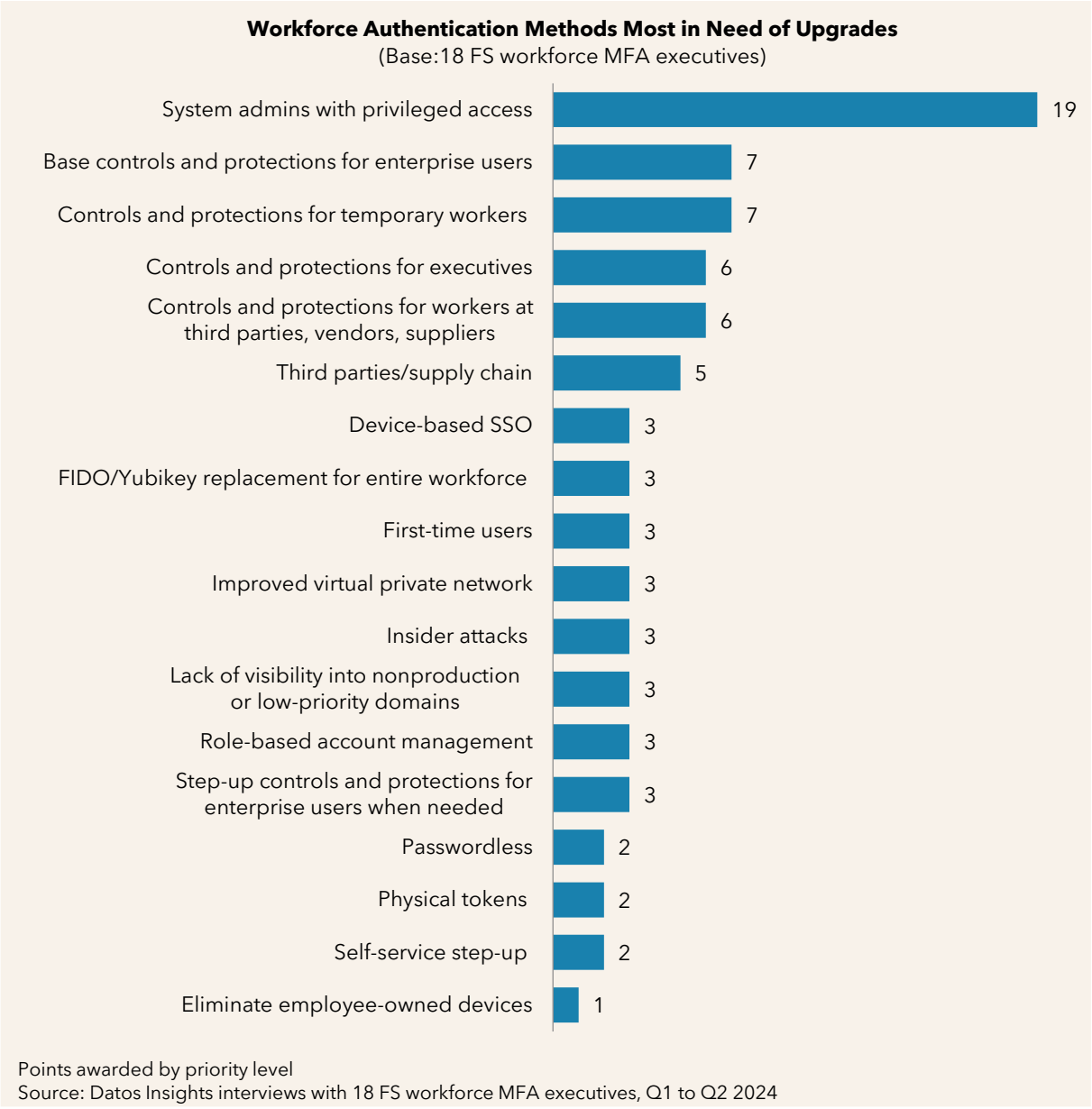
- **Supply chain risk from third parties was the second-highest-ranking cyber risk.** FS institutions leverage third-party software and third-party Software-as-a-Service (SaaS) applications as standard practice across the enterprise. The cyber risk introduced through third-party software and vendor SaaS is a severe concern for CISOs, especially as many third-party services operate with poor MFA, data hygiene, or operational controls.

- **Ransomware has made a comeback, ranking third.** With phishing or malware functioning as the means to successful access, ransomware (with encryption) and the so-called "extortion ware" (without encryption) infiltrations are on the rise. FS CISOs see ransomware as a top-three threat in 2024.

Workforce Authentication Most in Need of Upgrade

CISOs were asked to assess major portions of the workforce, current authentication solutions for each user category, and identify authentication solutions that most needed a security assurance upgrade (**Figure 3**). A point system was used to tabulate results.

Figure 3: Workforce Protections Most in Need of Upgrades



Points awarded by priority level
Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

Major findings and analyses are listed below:

- **Authentication supporting systems administrators were, by far, the most chosen solution to upgrade by CISOs.** This upgrade was strongly chosen despite the fact that most FS firms had already deployed PAM solutions with separate credential vaults to govern system admin access and behaviors. CISOs shared their PAM solutions and the degree to which these degree capabilities were implemented. CISOs understand that systems administrators have the greatest access and, hence, pose the greatest business risk if they are beaten in an attack, as well as the greatest opportunity to execute an insider attack if motivated to do so. Based on these results, this analyst believes that CISOs find current PAM solutions inadequate on their own to protect systems administrators and the business.

- **Authentication solutions for third-party vendor users also need security upgrades.** Many third parties are soft targets for cybercriminals in the modern age. CISOs know that vendors connecting to their enterprises are serious cyber threats to the business, warranting stronger MFA. This area can be challenging for the CISO. Because vendors are important to the business, FS firms are often reluctant to bring additional friction to the vendor channel. Regardless, this area represents a strong opportunity to improve security controls.

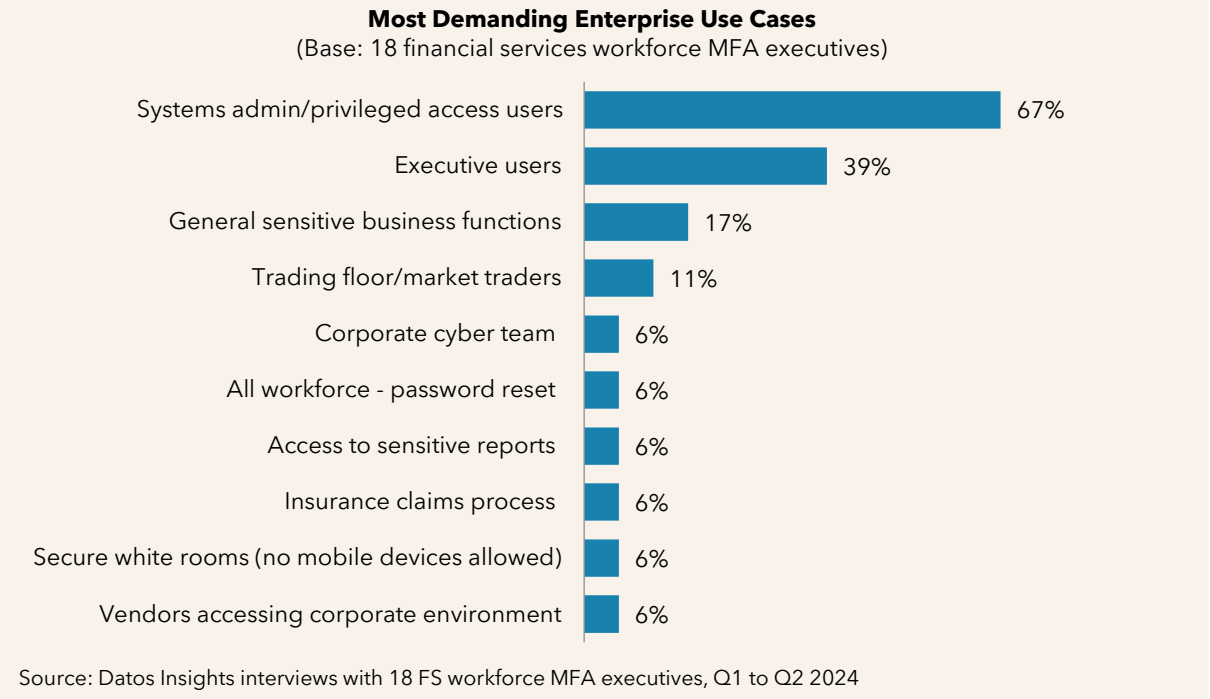
- **Base authentication controls experienced by all workforce users at every login attempt, as well as step-up controls for most users, are ripe for security upgrades.** Many CISOs reflected with some chagrin that progress has been made but that phishing-resistant MFA upgrades to base and risk-based controls are needed from their historical capabilities.

- **Authentication controls for executive users conducting sensitive business functions is also an opportunity area.** CISOs shared that their executives were protected via mitigating controls and frequent access reviews. However, none used advanced methods such as NG MFA to better protect important, top-of-the-house leaders from spear-phishing or ransomware attacks. This advisor thinks it is important for FS institutions to remediate this gap in 2024. Executives are increasingly under attack from cybercriminal teams, which are increasingly capable of adversarial AI-enabled attacks. Protecting these executives and protecting the business from an executive lapse seems critical in the modern age of cyber risk.

Most Demanding Enterprise Cases

CISOs were asked to identify their top enterprise cases that best fit the potential use of the NG MFA solution. Referred to as the "most demanding" enterprise cases, they were characterized by high business risks, which naturally warranted stronger MFA solutions (and justified their associated costs). **Figure 4** summarizes these results.

Figure 4: Most Demanding Enterprise Cases for Risk Reduction



Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

The primary findings follow:

- **CISOs once again selected systems administrators (67%) as the top opportunity for remediation.** High business risk through multiple cyberattack vectors, plus insider attack possibility, make these privileged users ripe foradvanced security methods such as NG MFA.
- **Executive users were identified by 39% of CISOs as appropriate for business risk reduction through capabilities such as NG MFA.** Many CISOs recognized the risk gap associated with executive-sensitive functions.
- **More broadly, CISOs assigned "most demanding" to any sensitive business function for potential improvement through NG MFA.** These included commercial banking

processes for FIs, investment traders, policy underwriters, and cybersecurity team functions.

Deployment for Third Parties and Customers

CISOs were asked to share their perspectives on how NG MFA solutions would be deployed to help their firm mitigate risk associated with third-party vendors and customers (consumers).

The severe business risks associated with third parties are well recognized by CISOs. A business model of "bring your own FIDO" was favored by most CISOs as the best approach to reduce risk for the third-party channel, bringing NG MFA into play for vendors without dictating nor reselling the solution. This analyst recommends the optional "we support your FIDO-compliant solution" model to address high vendor cyber risk and finds NG MFA a solid solution in this context. Leading FS firms must move beyond "all or nothing" MFA models and move to opt-in models if they desire to de-risk how vendor users access their enterprise. "Bring your own FIDO" does this.

The business risks and opportunities for customers are also noteworthy. Commercial customers have significant risks associated with FS interactions and seem well-suited for advanced authentication solutions. In the same opt-in spirit of "bring your own FIDO," this analyst views solutions such as NG MFA as attractive for commercial customers and some high-value retail customers.

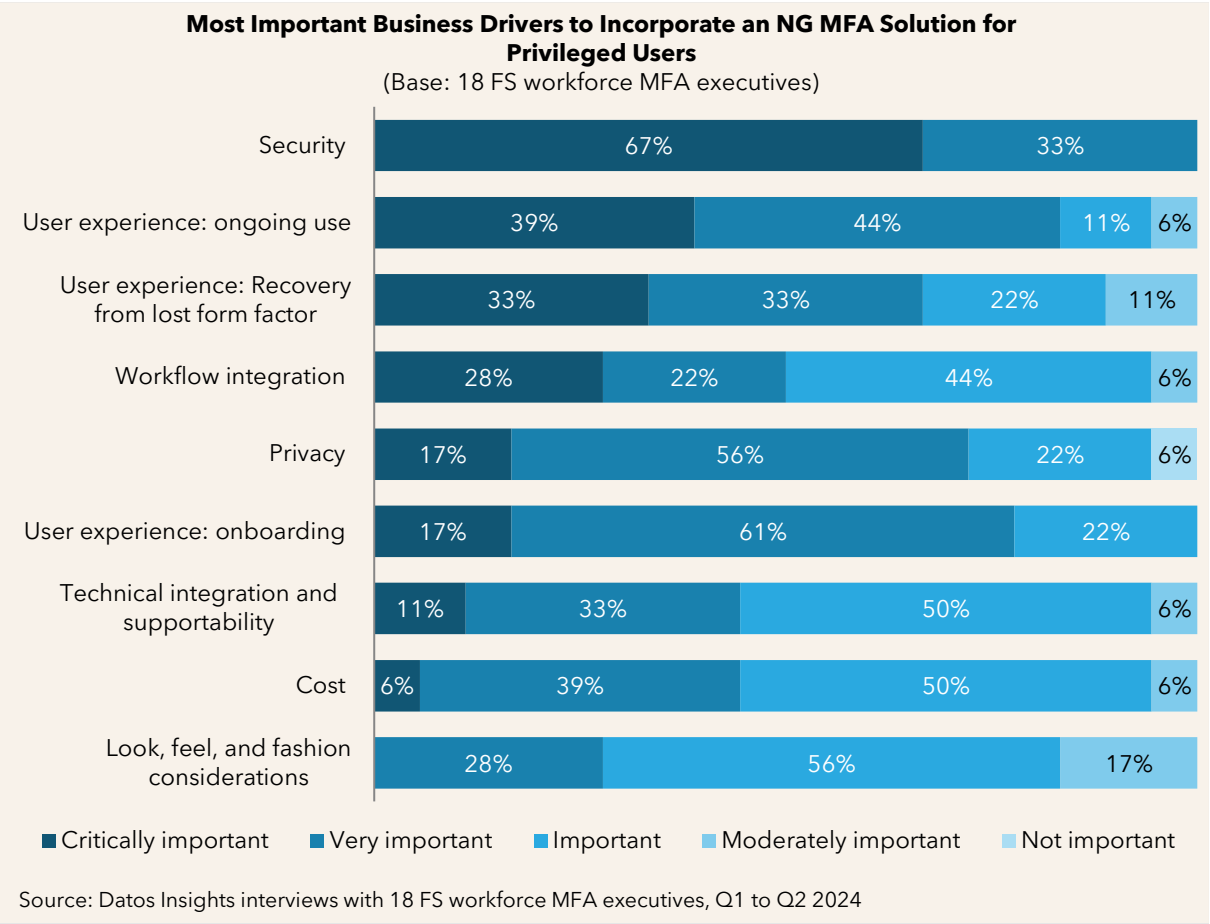
Operational View of Solution Capabilities

FS CISOs were given an overview of NG MFA solution capabilities and were asked to prioritize value contributors in the context of solution procurement and enterprise deployment.

CISO Priorities for Solutions Capabilities

The NG MFA solution has a set of robust capabilities. CISOs were asked to rate and prioritize nine categories in considering procurement and operationalizing the solution within their FS institution. These deep-dive discussions were very practical, exploring concepts and asking questions to understand specifics related to operating the solution in their organization. Summarized results are found in **Figure 5**.

Figure 5: FI Business Drivers for Unified Digital Banking/CIAM Solutions



Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

Primary findings from the research include the following:

- **Solution security is the top value driver for CISOs, who would not consider the solution if it did not possess premier security assurance.** Sixty-seven percent (67%) of CISOs rated security as critically important, and 100% of CISOs rated security as critically or very important. Premier security assurance is the primary value CISOs must recognize initially to consider the NG MFA solution.

- **Ongoing use is an important value driver for CISOs, with 83% rating it as critically or very important.** As more than one CISO shared, the solution simply needs to work every day, all the time. Because the solution deployment brings about a culture change within parts of the organization, ongoing ease of use is of high importance. Negative user experiences or difficulties using the solution undercut the overall success of NG MFA, as workers will tend to find other ways to accomplish their jobs without using the solution. The solution must elevate security (reduce risk) for the organization and must also be easy for workforce members to operate daily. Reviewing the solution, this analyst believes daily ease of use is driven by regimented user training, operational stability of the rings, and technical integration to enterprise workflows. Simple, operational ease of use is the primary lens through which CISOs will *seriously* consider using the NG MFA solution at their FS enterprises.

- **Other important capabilities for CISOs are recovery from lost rings, workflow integration, and onboarding ease.** Each of these valuable aspects contributes to overall ease of use. The recovery from a lost ring scenario relates to business risk when a workforce user loses their ring, the interim security policy the organization will enforce until the user receives their replacement ring, and the ease with which security or IT leaders effect these changes.

- **CISOs recognize user privacy is an important aspect of the solution.** Chief privacy officers are typically responsible for consumer privacy, but CISOs are also sensitive to privacy concerns. Questions surfaced in many discussions about where the ring biometrics are stored (user data never leaves the ring) and if the ring tracks user location (it does not). This analyst's assessment suggests the privacy narrative of the NG MFA solutions is very strong.

- **All participants viewed cost as having some importance, but it was not a primary consideration.** With initial workforce deployment limited to high-risk enterprise cases, CISOs assessed cost as eighth out of nine aspects.

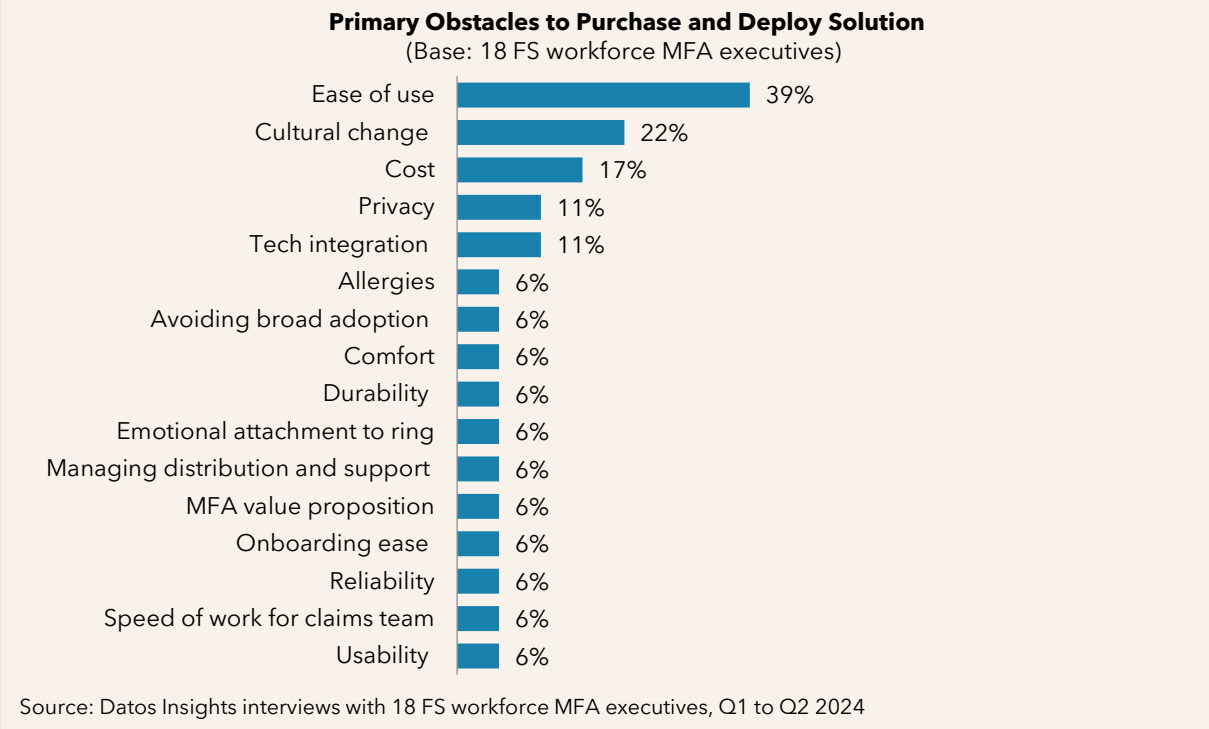
- **The wearable aspect of the solution can be expected to generate "look and feel" feedback, especially from executive users.** This analyst predicts executive users are most likely to express how the NG MFA ring feels to them. Getting the ring size right during the onboarding process is critical.

Potential Objections to Overcome

CISOs were asked to share their views of top potential objections to deploying the NG MFA solution for enterprise workforce users from their security professional perspectives and from the sponsoring executive perspective.

Figure 6 presents potential CISO objections/obstacles.

Figure 6: Potential CISO Objections



Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

Figure 7 presents potential executive objections/obstacles.

Figure 7: Potential Executive Objections

Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

Combining CISO perspectives with potential executive objections, three findings emerge:

- **Practical, daily ease of use and the cultural change initiated by deploying NG MFA were the top potential objections surfaced by CISOs.** These are intertwined considerations. Within the study interviews, CISOs assessed the demonstrated NG MFA capability as easy to use. They recognized the significant cultural change associated with NG MFA deployment at their firms and anticipated concerns from some peers and executives. In deeper discussions, CISOs emphasized the need for careful planning and socialization of the solution for these leaders. CISOs recognized the cultural challenges associated with lifting the enterprise workforce to a new level of security assurance and the standard aversions to change within the business. Still, they were highly intrigued by this pursuit and anticipated needing an expert vendor to partner with for deployment success.
- **The feel of the smart rings was highlighted for executive users.** Focusing on ring sizing during the user onboarding process is a key consideration. This analyst found this aspect delivered at high quality.

- **Other potential objections, including cost and privacy, were viewed as standard for deploying any new security solution.** These objections seemed easy to overcome with effective planning.

CISO Deployment and Budget Considerations

CISOs were asked to share how they envisioned the initial deployment of NG MFA and their budget support for such activities.

Initial Solution Deployment Preferences

Nearly all CISOs planned to introduce NG MFA to their security leaders first. Knowing these leaders would essentially become communicators of the solution to others, beginning solution deployment within the security organization follows standard practice. Security leaders would be asked to assess the ease of onboarding, use, and supporting processes.

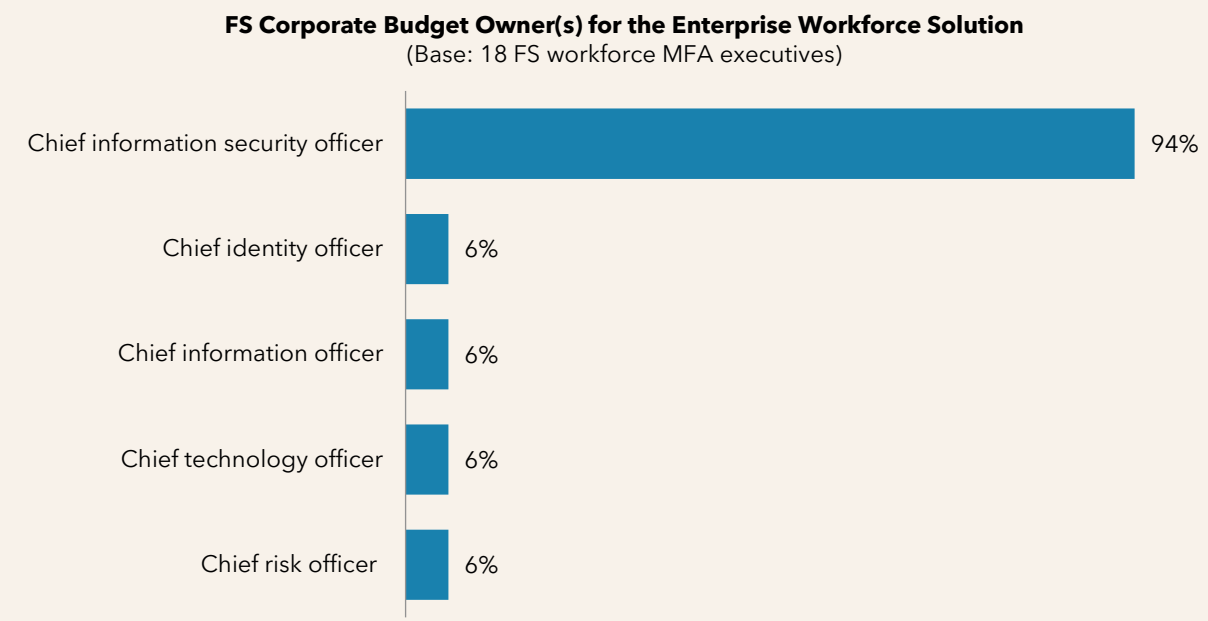
Most CISOs indicated solution deployment would immediately follow for IT systems administrators. These privileged users map directly to how CISOs identified top cyber risks to the enterprise, groups most needing MFA upgrade, and most demanding (attractive) enterprise cases (see Figures 1, 2, and 3).

Some CISOs indicated that specific executives might be targeted for initial solution deployment so that solution sponsorship would get its best foothold at the top of the house prior to subsequent deployments.

CISO as Budget Holder

CISOs were asked to share the title of the executive budget holder for NG MFA at their firm. **Figure 8** presents these results.

Figure 8: Budget Holders for NG MFA Solution



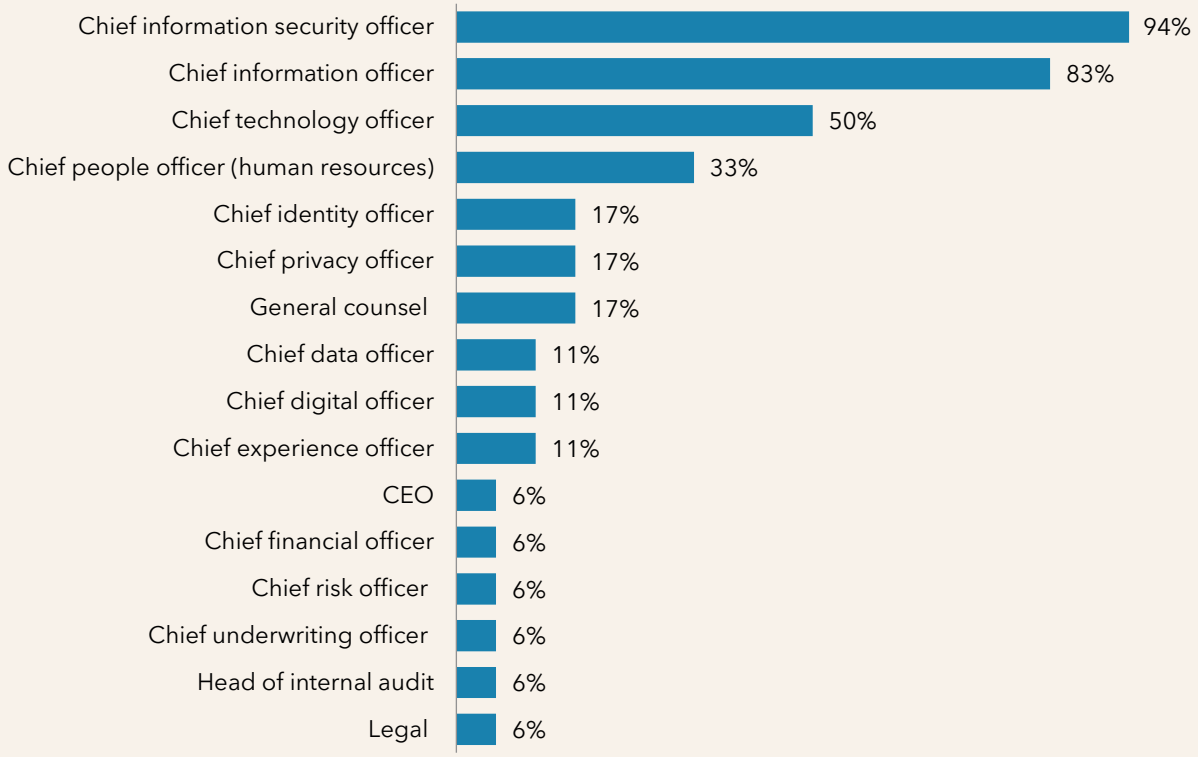
Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

Ninety-four percent (94%) of CISOs in this study asserted that they were the budget holders for solutions like NG MFA at their firm. These capabilities fall squarely into the CISO's remit. Though not a surprising result, it was affirming.

Budget Stakeholders

CISOs were also asked to share key executive stakeholders whose support they needed to procure and deploy NG MFA at their firm. **Figure 9** presents these results.

Figure 9: Budget Stakeholders for NG MFA Solution



Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

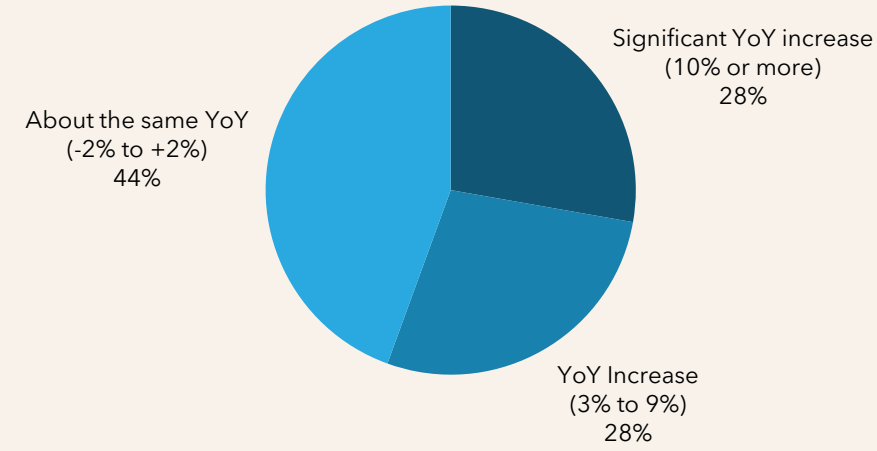
The firm's CISO was the top stakeholder identified by 94% of participants, followed by the CIO (83%) and the CTO (50%). These executives seem natural, given the nature of the solution and traditional CISO reporting. CISOs varied in whether their CIO or CTO was necessary to formally approve a purchase, an important executive partner for initial solution deployment, or, in some cases, both.

The executive responsible for human resources was also highlighted by 33% of CISOs, stemming from the aspect of cultural change the solution represents. Other executives were identified more as collaboration partners for initial solution deployment within the organization.

Budget Trending

CISOs were asked to share year-over-year (YoY) budget aspects for workforce authentication and access controls at their firm so that budget trending could be understood. Figure 9 compares YoY enterprise MFA budget changes from 2023 to 2024.

Figure 10: Enterprise MFA Budget 2024 vs. 2023

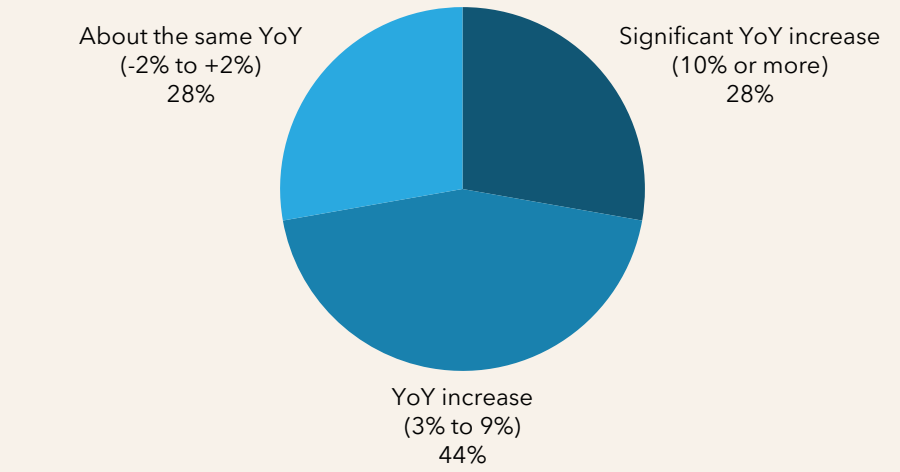


Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1-Q2 2024

These YoY budget results show strong growth for CISOs related to improving security assurance for their enterprise workforce. In 2024, 56% are operating with at least a 3% budget increase as compared to 2023, with 28% operating with a 10% or more YoY increase.

Figure 11 compares projected YoY enterprise MFA budget changes from 2024 to 2025.

Figure 11: Enterprise MFA Budget 2025 (Projected) vs. 2024



Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

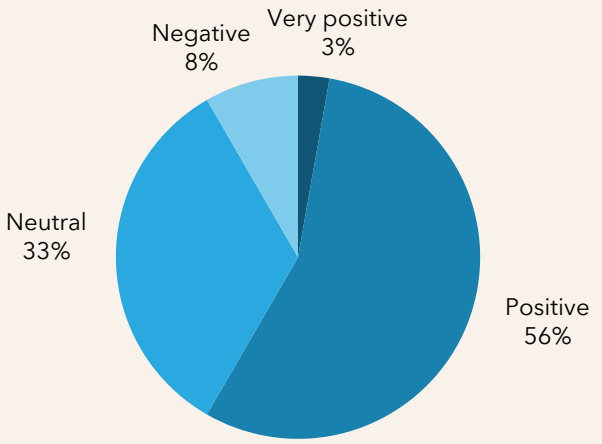
Looking forward to 2025, CISO budget forecasts are even stronger, with 72% operating with at least 3% YoY budget growth. In 2025, 28% expect to operate with a 10% or more budget growth for workforce authentication and access control solutions. This is a particularly robust budget season in support of advanced solutions such as NG MFA for the digital workforce.

Overall CISO Solution Impressions

Near the conclusion of each interview, CISOs were asked to provide an "overall impression" of the NG MFA solution, reflecting the practical nature of introducing this kind of solution for high-risk enterprise cases at their firm. Figure 11 presents these results.

Figure 12: CISO Overall Impressions of Deploying NG MFA

Q. What is your overall impression about leveraging this NG MFA solution to deliver more advanced protections for your business?
(Base: 18 FS workforce MFA executives)



Source: Datos Insights interviews with 18 FS workforce MFA executives, Q1 to Q2 2024

The top findings are included below.

- **Fifty-nine percent (59%) of CISOs assessed the solution as positive or very positive for deployment at their firms.** These CISOs were characterized by high intrigue and interest in understanding the solution in greater detail, mapping the solution against their top workforce security risks and needs, and holding a desire to pursue a proof-of-concept project.
- **Thirty-three percent (33%) of CISOs assessed the solution as neutral at present.** These CISOs saw "some positive" and "some negative" in the solution and held other high-priority workforce security improvements in plans for 2024.
- **Eight percent (8%) of CISOs assessed the solution as negative at present.** These CISOs were broadly skeptical about leveraging any wearable form factor for their workforce.

Conclusions

CISOs and workforce MFA leaders at FIs, insurers, and FS services firms should keep in mind the following takeaways:

- CISOs need to deploy phishing-resistant MFA for their workforce users: Many market solutions exist. With generative AI enabling more sophisticated attacks, elevating business risk and recovery costs, CISOs should seek solutions that can demonstrate premier or "next-generation" defenses especially for systems administrators, executive users, and other business-critical sensitive functions.
- **Map advanced solutions such as NG MGA against the top assessed cyber risks.** No single solution reduces all risks, but advanced solutions like NG MFA significantly mitigate the phishing vector and ransomware risks prevalent in the market. Adversarial AI is increasing these risks.
- **Break the perceived glass ceiling for cultural change.** The criminal use of AI is amplifying business interruptions and financial losses from cyberattacks. Business risk is rising. Innovative solution deployment needs to accelerate for many firms. The internal tendency within some organizations to avoid change must be overcome for the sake of the business.
- **Start small.** Enterprisewide deployments of advanced solutions are possible, but considering smaller deployments to address high-risk areas of the business can be more prudent. This research highlights security teams and systems administrators as top candidates for initial solution deployments.
- **Find domain expertise.** Digital identity and advanced MFA skill sets are severely lacking in the market. Many FS firms will need to seek external sources, including industry consultants and solution providers for seasoned domain experts.

About Datos Insights

Datos Insights is an advisory firm providing mission-critical insights on technology, regulations, strategy, and operations to hundreds of banks, insurers, payments providers, and investment firms—as well as the technology and service providers that support them. Comprising former senior technology, strategy, and operations executives as well as experienced researchers and consultants, our experts provide actionable advice to our client base, leveraging deep insights developed via our extensive network of clients and other industry contacts.

Contact

Research, consulting, and events:

sales@datos-insights.com

Press inquiries:

pr@datos-insights.com

All other inquiries:

info@datos-insights.com

Global headquarters:

6 Liberty Square #2779
Boston, MA 02109

www.datos-insights.com

Author information

John Horn

jhorn@datos-insights.com