CYBER READINESS
INSTITUTE

Unlocking MFA Adoption: Why Small and Medium-Sized Businesses Must Act Now to Strengthen Their Cybersecurity

A new Cyber Readiness Institute global survey reveals that while U.S. SMBs are embracing Multifactor Authentication (MFA), global adoption remains alarmingly low. The 2024 report outlines critical steps needed to drive MFA adoption, protect supply chains, and secure digital assets worldwide.

Multifactor Authentication (MFA) is widely recognized as one of the most effective defenses against cyberattacks, adding vital layers of protection that can significantly reduce the risks of unauthorized access into organizations and their supply chains. As cyber threats continue to increase in frequency and sophistication, MFA is an essential tool to help small and medium-sized businesses (SMBs) protect their own assets and be more trusted partners to other businesses.

However, MFA and other aspects of cyber readiness at times can be intimidating and confusing to businesses, especially those that can't afford internal IT staff. That is why it is crucial to understand just where SMBs stand regarding the awareness and implementation of MFA, and what steps are necessary to encourage widespread adoption by them.

The Cyber Readiness Institute (CRI) has been tracking MFA adoption since 2022. Our latest global survey of nearly 2,300 SMBs[1] shows most SMBs remain unaware of the tool and do not employ it (despite overwhelming evidence of its benefits). Many SMBs are reluctant to require MFA for internal use, or for their customers and suppliers. This hesitation is often due to cost concerns, resource constraints, and a lack of understanding of the security benefits. As a result, many global SMBs and their supply chains remain vulnerable to cyber threats that could otherwise be mitigated.

WHAT IS MFA?

MFA requires users to verify their identity through two or more factors, such as something they know (a password), something they have (a smartphone or security token), or something they are (biometrics like a fingerprint or facial recognition). For instance, after entering a password, users might receive a code or notification on their phone to confirm their identity.

This additional step makes it much harder for attackers to gain access, even if they've stolen passwords. According to the U.S. Cybersecurity Infrastructure and Security Agency (CISA),[2] MFA users are 99% less likely to be hacked.

CRI's 2024 survey reveals MFA implementation among SMBs worldwide has declined from 46% two years ago to 35% today, even as U.S. businesses far outpace their global counterparts in MFA adoption over the past 12 months. These findings underscore the need for more educational outreach and support to help businesses understand MFA's value and implement it effectively.

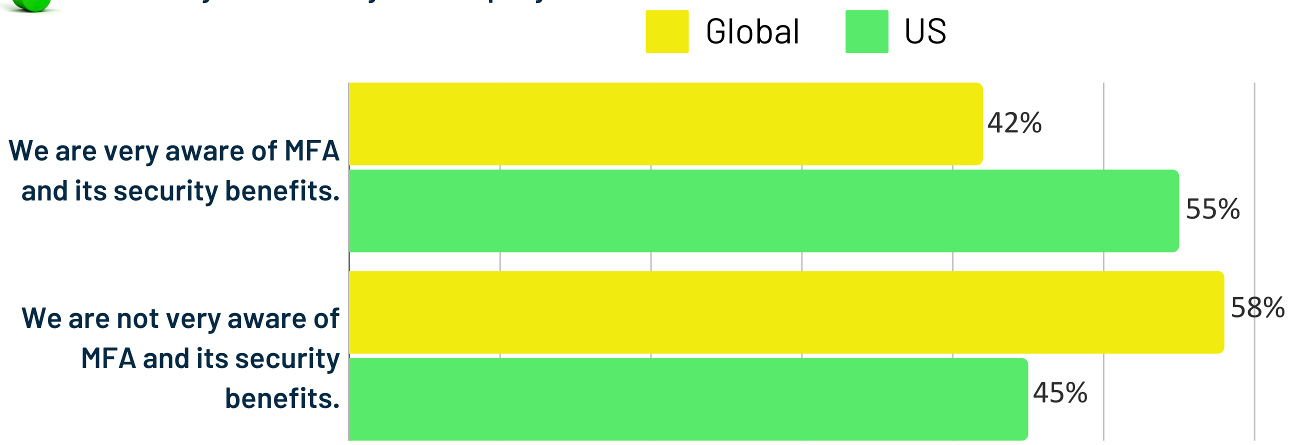
[1] The CRI 2024 global MFA survey was conducted through Survey Monkey, reaching 2274 SMBs worldwide. All global and worldwide survey data in the report include responses from U.S. SMBs.

[2] CISA: Multifactor Authentication.

The MFA Gap: Key Findings

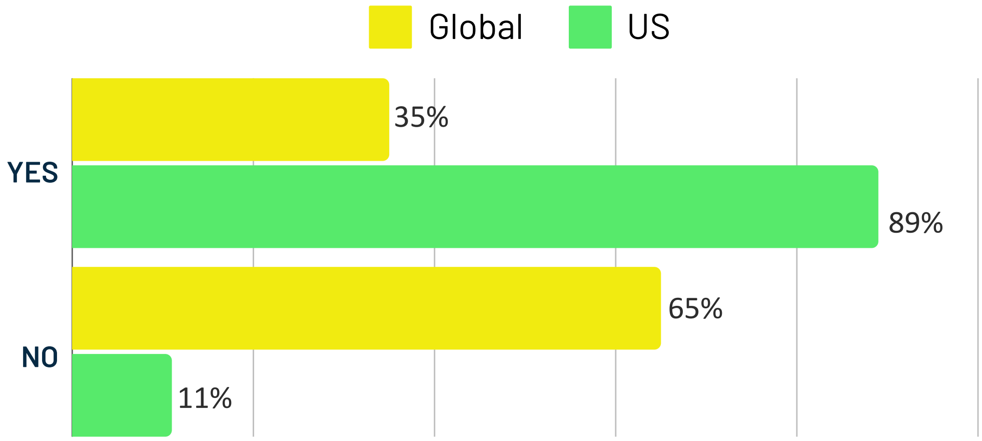
Awareness and Implementation Remain Low: Nearly six in ten SMBs (58%) remain unaware of MFA's critical role in securing their businesses, contributing to low implementation rates (35%) worldwide. This lack of awareness is a significant roadblock to wider adoption.

The following best describes the level of awareness you have of MFA and the related security benefits at your company.



Source: CyberReady Institute MFA Oct 2024 (Global N = 2274, US N = 394)

Does your business implement MFA?



Source: CyberReady Institute MFA Oct 2024 (Global N = 2274, US N = 394)

Challenges Faced by Companies Implementing MFA: Among SMBs that have adopted MFA, funding for the tools (38%) and a lack of technical expertise needed to choose solutions that would be right for their unique business needs (37%) were among the top challenges to implementation.

Few Require MFA Use Internally or by External Partners: An overwhelming nine out of 10 SMBs (85%) do not require the use of MFA by customers or suppliers connecting to their systems. And less than one in five (17%) of SMBs worldwide have internal cybersecurity policies requiring the use of MFA within their organizations.

Communications Breakdown: Nearly half (47%) of SMBs worldwide that use MFA provide information to employees on the importance of the tool, and four out of 10 offer instructions on use. However, only one in three (32%) send employees frequent communications reinforcing the importance of MFA, and only one out of five (20%) send regular training communications to aid employee use of MFA.

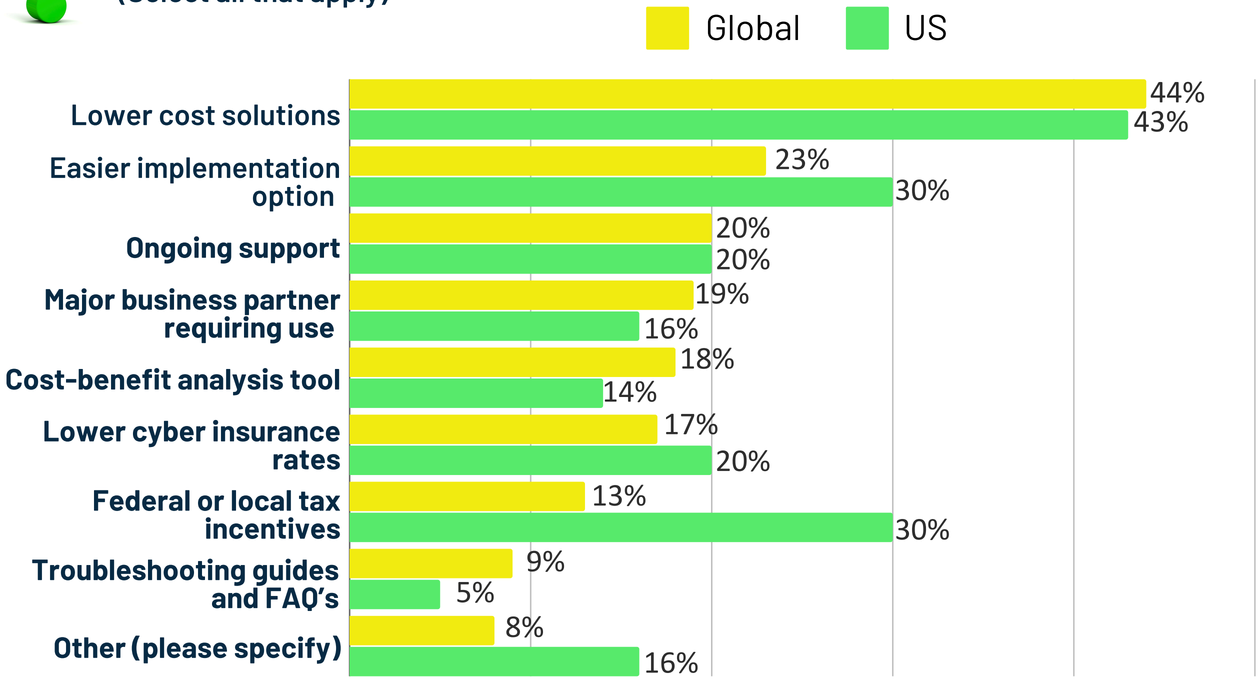
Reasons Companies Do Not Implement MFA: Nearly four out of 10 (37%) SMBs worldwide indicate investing in MFA is not a top priority for them. Other reasons for not implementing MFA include:

- Lack of understanding of security benefits (22%)
- Lack of funding (20%)
- Lack of in-house technical expertise to research solutions (18%)

Plans to Use MFA in the Future: There remains a significant hurdle to convince non-users to implement MFA. Over six out of 10 SMBs worldwide (61%) indicate they see no need to use the tool in the future.

Incentives for Adoption: Among SMBs worldwide that have yet to implement MFA, cost is the primary barrier to adoption. Even though software providers have begun to bundle MFA with their offerings, it appears many SMBs are concerned about related costs (technical expertise required to rollout the tool, for example) and still view it as a resource strain rather than a security investment. SMBs cite other significant factors to incentivize broader adoption of MFA including streamlined integration processes, ongoing technical support, and a requirement by major business partners.

Which of the following would incentivize your organization to require the use of MFA? (Select all that apply)



Source: CyberReady Institute MFA Oct 2024 (Global N = 747, US N = 44)

U.S. SMBs Outpace Global Counterparts Closing the MFA Gap

The 2024 Global MFA survey reveals significant differences in MFA awareness and implementation between U.S. and SMBs worldwide.

U.S.-based SMBs report a dramatic increase in MFA implementation, with nearly nine out of 10 SMBs (89%) indicating they use MFA, a huge increase from only 53% last year. Despite this progress, awareness of MFA among these organizations paradoxically remains at earlier levels of 55%.

What's more, the survey data indicates a seeming disconnect between how U.S. and non-U.S. SMBs approach MPA requirements for customer and partner connections. More than nine out of 10 U.S. SMBs (95%) using MFA internally, require its use by customers and suppliers accessing their systems, reflecting a proactive approach to securing their business ecosystems. However, only 15% of SMBs worldwide require MFA for customers and suppliers connecting to their systems.

One area where the data indicates U.S. SMBs and their global counterparts align: Business that have not implemented MFA see no need to change their view. Seven out of 10 of U.S. companies (70%) say they have no plans to implement MFA in the future, while 61% of SMBs worldwide do not have plans to use the tool in the future.

A Call to Action: Accelerating MFA Adoption

To drive wider adoption of MFA and enhance cybersecurity practices across SMBs worldwide, CRI has identified four critical areas that must be addressed: communication; cost; internal and external policy requirements; and resources and tools.

1. Communication: Spreading Awareness and Education

Despite overwhelming evidence of MFA's effectiveness in preventing cyberattacks, many SMBs remain unaware of its benefits. The cybersecurity landscape is increasingly complex, and businesses are often overwhelmed by technical jargon, leaving them uncertain about where to begin.

Key Actions:

- **Targeted Awareness Campaigns:** Government agencies, industry associations, non-profit organizations, and cybersecurity firms must continue to collaborate to launch targeted, ongoing campaigns that clearly explain MFA's role in securing digital assets, emphasizing how it can serve as a simple but powerful safeguard to the growing risks of cyberattacks.
- **Simplified Messaging:** MFA should not be seen as a complicated or optional tool. The messaging must present MFA as a straightforward, accessible, and effective defense mechanism for businesses of all sizes. Clear, non-technical language should be used to ensure the benefits are easily understood by business owners, not just IT professionals. We need to seize the moment as most people, in their personal and business transactions, are already familiar with the tool, although they may not even know they're using MFA.
- **Success Stories:** Sharing case studies of businesses that have successfully implemented MFA can serve as powerful examples. These stories can demonstrate how adopting MFA has helped reduce cyber threats, thereby motivating others to follow suit. Hearing the experiences of other small business owners, will also allay some of the concerns SMBs cite in the survey data.

By creating a clearer, more compelling narrative around MFA, more SMBs can be encouraged to integrate this vital security layer into their operations.

2. Costs: Reducing Financial Barriers to Adoption

For many SMBs, the perceived cost of implementing MFA is a significant barrier to adoption. While MFA is increasingly a feature included in many software products, it is not yet a widespread practice. There are also ancillary costs such as managing deployment throughout an organization as well as ongoing maintenance, causing SMBs to view MFA as an additional expense rather than an investment. This perception is particularly strong in businesses with limited resources, where cybersecurity may not be prioritized. However, the reality is that the cost of a cyberattack—whether through data breaches, financial losses, or reputational damage—can far outweigh the initial outlay for MFA. According to a 2024 survey by Microsoft,[3] cyber-attacks cost SMBs more than $250,000 on average and can range up to $7,000,000, a financial hit most SMBs simply cannot afford.

[3] New research: Small and medium business (SMB) cyberattacks are frequent and costly.

Key Actions:

- **Bundling MFA with Existing Software:** The more secure features of MFA should be included in software purchases at little to no extra cost. Clear communication about the inclusion of MFA in existing packages can also help businesses realize the technology is available to them without additional expense.
- **Government and Corporate Incentives:** Tax incentives, grants, subsidies and preferred supplier status could also encourage SMBs to adopt MFA. Some corporations operating global supply chain incentive their business partners to adopt MFA by offering preferred supplier terms. Government procurement services should do the same.

Through these financial incentives and cost-cutting measures, SMBs are more likely to see MFA as an affordable and necessary security measure.

3. Internal and External Requirements: Making MFA a Standard Practice

One of the surprising findings of CRI's latest survey is that less than one in five SMBs require MFA as part of their internal cybersecurity policies—even in countries such as the U.S. where use has skyrocketed. This gap leaves critical business systems and data vulnerable to cyberattacks, despite growing awareness of the risks. Moreover, only a small percentage of SMBs worldwide require MFA for customers, suppliers, or external business partners, further exposing their ecosystems to potential threats.

Key Actions:

- **Updating Internal Policies:** As cyber threats increase, companies should incorporate MFA as a required component of their internal cybersecurity guidelines for accessing all critical systems and sensitive data, especially for high-privilege users. Internal compliance can be driven by leadership, IT departments, and/or cybersecurity teams championing the importance of MFA and educating staff on its necessity.
- **Setting External Requirements:** Businesses should insist on MFA in all dealings with their customers, suppliers, and partners. This commitment would ensure more secure supply chains and reduce the risk of breaches originating from third-party access. Larger corporations and supply chain operators can lead by example, requiring their partners to use MFA as a condition of doing business. SMBs are more likely to adopt MFA if it becomes a requirement for maintaining relationships with key partners.

Building MFA into the internal and external operations of businesses, and making it a standard requirement in supply chains, will ensure more comprehensive cybersecurity across industries.

4. Resources and Tools: Supporting SMBs with Clear Guidance and Technical Help

Many SMBs do not have the in-house expertise or resources to implement MFA effectively, leaving them unsure of how to start. Technical support and clear, practical guidance are critical to helping businesses understand MFA's value and how to integrate it into their cybersecurity strategies.

Key Actions:

- **Educational Resources:** SMBs need access to simplified, easy-to-follow guides that walk them through the MFA implementation process. This could include tutorials, best practices, and step-by-step integration instructions for various platforms. Cybersecurity organizations, non-profits, industry bodies, and government agencies should continue to provide comprehensive toolkits designed to educate business owners about MFA's benefits and setup processes.
- **Technical Support:** Many businesses lack the internal IT support needed to manage MFA post-implementation. Offering ongoing technical assistance—whether through third-party vendors, government programs, or industry associations—can help businesses resolve issues as they arise and ensure the long-term effectiveness of their MFA solutions.
- **Streamlined Integration:** To further encourage adoption, software providers should offer MFA solutions to integrate seamlessly into existing systems. Pre-configured options and user-friendly dashboards can simplify the deployment process, reducing the need for extensive technical expertise.

To help SMBs better understand and implement MFA within their cybersecurity strategies, CRI has compiled a list of some comprehensive resources designed to support businesses at every stage of their MFA journey, from initial awareness to advanced implementation:

- GCAToolkit for Small Businesses
- Kubikle Series
- Microsoft ASP.NET MFA Guide

Conclusion: Act Now to Secure Your Digital Future

MFA is no longer a luxury or optional security measure—it is a fundamental necessity in today's digital landscape. The time for SMBs to act is now. By addressing the challenges around communication, cost, requirements, and resources, businesses will be better equipped to prioritize MFA, protect their assets, and build resilience against future cyber threats.

The longer SMBs delay implementing MFA, the greater the risk they face. Businesses adopting MFA not only safeguard themselves but also contribute to more secure business relationships and a more resilient global economy. By prioritizing MFA adoption today, businesses can protect their customers, partners, and supply chains from the ever-evolving threat of cybercrime.

For the survey data, please visit: 2024 Global MFA Survey Insights.