
# Tips on implementing multi-factor authentication (MFA)

**The current cyber threat environment has increased the focus on authentication measures to help ensure data and systems are accessed by the appropriate people. The proliferation of usernames and passwords on the dark web has forced the need of different factors of authentication beyond the common password. Enter multi-factor authentication (MFA).**

Authentication factors include the following:

- Something you **Know** (password or secret answer)
- Something you **Have** (smartphone, security token with ever-changing numbers)
- Something you **Are** (biometrics — facial recognition, fingerprint)

Considerations on which factors to use include inherent risk, features/cost, integration ease, user experience, and of course, cost. We break down these considerations and others.

**All factors are not created equal.** Some factors are better than others and some should not be used in today's environment. It is the author's opinion that the following are security considerations for common factors:

- **Lower security**: SMS text messages, email — these should only be used as a last resort, if at all
- **Better security**: Authenticator push, time-based one-time passwords
- **Best security**: Facial recognition, fingerprint, security token, smart cards

### Make sure it's "true" multi-factor authentication

Using something you know (password) with something you know (secret question/answer) is easily susceptible to attacks and is not considered "true" MFA. Stronger security dictates using factors from two or more of the categories above (know, have, are).

### Apply the appropriate factor based on the risk level

Many companies layer the types of authentications — maturing from a "defence-in-depth" posture to "zero trust," where different types of authentications are needed for different applications or data access. Remote VPN access may require an authenticator push, while more privileged access, say to the wire transfer application, requires a physical security token and perhaps another factor as well.

### Features/cost

When choosing an MFA platform, the analysis should include consideration of features such as analytics and reporting, user onboarding and experience and integration with existing applications. More expensive platforms may provide richer features and more control where MFA is applied. However, it could be that a less expensive platform is appropriate according to the organization's requirements.

### Train the users

User training should be considered mandatory, with refreshers provided at least on an annual basis. If it is a new MFA rollout, think more on the enhanced rigor of a marketing campaign. Other considerations include:

- Let users know that today's environment requires a higher level of security than just passwords.
- They should understand that if they receive "push requests" that they did not initiate, especially at odd hours, they should contact the security department, as it is likely their username and password combination has been compromised. These are known as MFA bombing or MFA fatigue attacks.
- Most importantly, they need to know that today's attacks revolve around social engineering. Attackers will ask for the code or try to get the user to activate the push authentication.

### Periodic review

As with any security control, it is important to periodically review the environment to help ensure MFA is applied to the appropriate assets and at appropriate measures. Keep and review metrics on failed logins, denied privilege escalations and service desk calls related to MFA.

### More questions?

These are just a few of the considerations when implementing multi-factor authentication. If you would like further guidance, please contact the WTW Cyber Risk Solutions Team.

**The WTW FINEX Cyber Risk Solutions (CRS) Team offers a range of customized consulting solutions to ensure your organization can cost effectively navigate the ever-evolving cyber risk landscape and consistently achieve your core business objectives.**

- We are former Chief Information Security Officers (CISOs) with a deep commitment to your success. We understand your business requires a tailored approach to properly identify, assess, and prioritize your cyber risks so you can effectively optimize allocation of budget and resources.
- With a clear lens on the cyber threats of today and those yet to come, we offer flexible tailored consulting services designed for you and your unique business needs.
- CRS tailored services can be delivered on-site or remotely, providing practical, actionable solutions and C-Suite-ready reporting containing valuable quantitative and qualitative insights.

### Cyber Risk Solutions North America

Our team of expert consultants bring diverse skills from technical, military, legal, business and risk management backgrounds.

Please contact us for more information on any of our tailored services.

#### North America contacts

**Sean Scranton** CISSP, CPCU, RPLU+, CISM, CISA
CRS Team Lead
+1 309 322 5133
sean.scranton@wtwco.com

**Jonathan Davies** C|CISO, CISSP, CCSP
Cyber Risk Consultant
+1 702 582 4300
jonathan.davies@wtwco.com



### About WTW

At WTW (NASDAQ: WTW), we provide data-driven, insight-led solutions in the areas of people, risk and capital. Leveraging the global view and local expertise of our colleagues serving 140 countries and markets, we help you sharpen your strategy, enhance organizational resilience, motivate your workforce and maximize performance. Working shoulder to shoulder with you, we uncover opportunities for sustainable success — and provide perspective that moves you. Learn more at wtwco.com.

wtwco.com/social-media


WTW-163030/10/24

wtwco.com