CORVUS | wingman Insurance

Tip Sheet: Multi-factor Authentication

Carriers increasingly require insureds to implement multifactor authentication as a subjectivity for a cyber liability policy.

What can you expect from the process and how can you help your clients to minimize disruption? Find out here.

What is MFA?

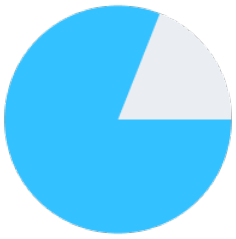
Multi-factor Authentication (MFA) is an authentication method that requires the user to provide two or more credentials in order to gain access to an account. Rather than just asking for a username and password, MFA requires one or more additional verification factors unique to the individual, which decreases the likelihood of a successful **cyber attack**.

Picture yourself at an ATM withdrawing money from your bank account. Your debit card *(something you have)* is one authentication factor. However, to access your account, you also need to enter the PIN that is associated with your debit card. Your PIN *(something you know)* is your second authentication factor.

Another common example nowadays is with access controls for online banking. In order to log into your online bank account from a new device, you must provide your username and password *(something you know)* along with another factor, such as a one-time passcode on an authentication app on your cell phone *(something you have)*. As cellphones incorporate biometric information, facial recognition (something you are) may be that additional factor.

Credentials may include:

- Things you know*:*
  a password or personal PIN
- Things you have*:*
  a badge or cellphone
- Things you are*:*
  biometric information such as fingerprints or facial recognition



81% of data breaches
in recent years are attributed to password compromises

Why is it important for cyber security?

Password compromises have accounted for **81 percent of data breaches** in recent years. There are limits to what a single password can do.

Rather than asking for a single password that hackers and cyber criminals can gain access to, this adds an additional layer of security. MFA **helps protect** against unauthorized access, data breaches and password-based cyber-attacks.

Where should it be implemented?

MFA is recommended to be implemented across:

- all remote access to data or the environment *(email, VPN, etc.)*
- for access to cloud and on-premises applications
- for any additional applications *(internal or external)* that contain personally identifiable information *(PII)*
- internal activity with privileged users *(owners of a credential that has admin access locally to a part of the system or domain-wide across many devices or servers)*

In plain English, companies should look to secure **any remote access points to their systems or data** with MFA. Internal usage of privileged accounts, such as local administrators or domain administrators, should be also secured with MFA where possible.

Some Factors are Stronger than Others

Cybersecurity professionals have long advocated that two-factor authentication utilizing text messages (SMS) is less secure than other methods.

The US government stopped using **SMS authentication in 2016** — and encouraged others to do the same. Since then, there have been successful breaches across organizations that still utilize this less secure variation of MFA.

There are countless ways for criminals to bypass SMS authentication, some more complex than others, **but opt for utilizing MFA apps like Duo, Google Authentication, or Microsoft Authenticator** if you're using a smartphone as a means to enable MFA for your organization.

MFA is Not the End-All-Be-All

MFA is an important preventive measure to take to avoid security breaches, but it is not an all-encompassing solution to protect an organization. As noted above, there are weaknesses with SMS-based authentication — and even the most secure forms of MFA have limitations.

For example, if an employee's personal computer was already compromised and they were utilizing a VPN to work from home, **MFA may not prevent malware** spreading throughout the corporate network . Additional external defenses would be necessary for further risk mitigation.

What does an MFA roll-out involve?

The timeline and cost of implementing MFA is dependent on several factors, like the size of your organization, the email provider and other technology platforms you're using, and how you plan to introduce the concept to all of your employees (from stakeholders to the IT department). In some cases, we've worked with policyholders who were already using a system, like Microsoft O365, that has MFA built in; it would only be a slight exaggeration to say that the process for implementing MFA at these organizations is as easy as flipping a switch. In other organizations, with many overlapping technology platforms and access points that have accumulated over time, implementation can be a bit more involved.

While the ultimate goal of MFA implementation is to eventually cover all users across your systems, it's good to prioritize where to begin based on the risk level to the organization. Starting with administrative (and high-risk) accounts has two key benefits: privileged accounts have the greatest security impact, and you can use what you learned in the roll-out with senior leaders to aid in deploying to the next round of employees. As you consider what systems require user log-in, recognize where you'll need to update (or replace) older infrastructure that doesn't support **modern authentication**.

The Price of Implementing MFA

While cost can be what holds some back from adding further security measures, MFA is an affordable option to further protect your organization.

Notably, through Microsoft O365 and Google Workspace, there are no additional costs to implement multi-factor authentication.

Getting Started

Looking for hands-on help with MFA implementation? Our consults with blue-chip vendors can help.

vCISO Services from Corvus aim to help organizations dig deeper into specific issues and find the right offering to meet their needs. The process begins with a free, no-risk consultation call to explore options. Any further services selected are offered at an exclusive discounted rate.

Visit **corvusinsurance.com/vciso-services** and fill out the form to get started, making sure to select "Multifactor Authentication Consult"

About Corvus

Corvus is reimagining commercial insurance for a digital world by making insurance smarter, companies safer, and brokers more successful. Corvus empowers brokers and policyholders with actionable insights to mitigate complex risks and reduce losses through the CrowBar digital platform, smart insurance products, and premier risk management services. Corvus is the world's largest specialty commercial InsurTech company.

Resources:

What is MFA (OneLogin)

The Importance of MFA (Tetra Defense)

Not all Two-Factor Authentication is Created Equal (LMG Security)

Microsoft Office 365 Security Best Practices to Protect Your Organization (LMG Security)

The Importance of Multi Factor Authentication in Cybersecurity (Veridium)

MFA Best Practices (Centrify)

How to implement Multi-Factor Authentication (MFA) (Microsoft)