



TRAVELERS BULLETIN SPECIAL EDITION 2021

Multi-Factor Authentication Special Edition 2021

Multi-Factor Authentication (MFA) requires the user to provide two or more methods to verify their identity in order to access a resource. Instead of just asking for a username and password, MFA requires one or more additional verification factors, which decreases the likelihood of a successful cyber-attack. Solely having a username and password can leave you vulnerable to brute force attacks and can also be stolen by threat actors. Enforcing the use of MFA in a business can increase confidence that your company is safer than it was.

MFA comes in many forms; some use biometrics such as fingerprints to verify a user, others can use physical hardware keys, while the most common form of MFA is likely to be one-time passwords. One-time passwords are 4+ digit codes which are sent to a user's previously confirmed email, phone number or application. A new code can be generated either periodically or each time an authentication request is submitted. Another type of MFA which is starting to be used is location-based verification. This usually looks at a user's IP address or geo-location and if the information does not match the whitelist (a mechanism which explicitly allows some identified entities to access a particular privilege or service), it can block the user from accessing the site. Adaptive Authentication is another form of verification that can be used for MFA. Adaptive Authentication analyses additional factors when a user tries to log in and uses these values to assign a risk level associated with the login attempt. This can be based on a multitude of things such as location; the time of day and what information is trying to be accessed; the kind of device used; and whether a connection is via a private or public network. The answers to these questions determine whether a user is required to provide an additional authentication factor or whether they will even be allowed to log in. Any effective and enforced Multi-Factor Authentication strategy will undoubtedly save any organisation time and money in the future.

“Some smaller businesses have expressed concerns over the costs or IT time it takes to implement MFA, which really is marginal in comparison to a cyber event that could leave their systems unavailable for days, possibly weeks, and eventually cost a lot more in the long term. For these companies, they should really consider the short-term pain for the long-term gain.”

Lisa Farr
Cyber Underwriter,
Travelers



In a recent dark web audit conducted by the Digital Shadows Photon Research team, it was revealed that there are currently more than 15 billion pairs of stolen credentials from over 100,000 data breaches which have been leaked online. Of this 5 billion are said to be completely unique. With an ever-increasing number of data breaches per year, it is essential to maintain strong account security settings across all accounts. In the absence of MFA, if a hacker discovers a pair of leaked credentials online for an Ebay account for example, they can simply get on to the account, unless the password has been changed, and have full access to everything on the site. They can then begin to use those same login details to attempt to access other personal accounts belonging to the victim, in a method known as password spraying.

Multi-Factor Authentication would prevent a threat actor from being able to access any accounts even if they had managed to successfully find a username and password, unless the authentication method had already been compromised (for example, the threat actor is in possession of the email login credentials used to receive a one-time password to authenticate access to an account).

With over 10 billion leaked passwords being used across multiple accounts, threat actors are well equipped to exploit an ever-increasing number of victims online. Therefore, it is critical to ensure that unique passwords are used across all accounts associated to a professional email address or phone number. Passwords should be updated regularly to ensure maximum protection against possible threat actors. Password managers such as BitWarden or LastPass are free and can be useful to store passwords. The user must remember a

master password which is required to access the list of credentials. From this list, the user can store and add login credentials for any professional accounts they may use and simply copy and paste passwords across when required for a specific account.

A recent survey, conducted by the company LogMeIn, identified that 91% of people know that reusing passwords is insecure, however, 62% of users still use the same password across their work and personal email accounts anyway. This presents a clear vulnerability in the systems of any organisation unable to adhere to strict password and IT security policies. A unified response is needed from all employees in order for an organisation to make any real change to be cybersecurity. MFA should not just be used for administrator or privileged accounts, as any account with access to critical company data, applications and systems can be exploited by threat actors to gain control over an organisation's network and data. Companies are only as secure as their weakest link in security, so a coordinated effort is needed from all employees. The end goal of MFA is to enable it for all users, on all company devices, and for it to be easily used. However, that will not happen on day one.

It is recommended that IT teams, for companies installing MFA, ensure that all employees are using the same method or app of authentication to save time when resolving issues in the future. It is important to be clear from the start what you are intending to protect, what MFA technology to use and the impact on employees. If prior planning is not thorough, MFA deployment may be detrimental to a business and grind daily operations to a halt due to complaints from users. Finding a solution that is right



for the specific business is key. Solutions should be easy to deploy across all users, work well alongside existing IT infrastructure and be easy to manage allowing administrators to react quickly to end-user problems.

MFA can be free to install, however, it can produce challenges for companies with regards to the logistics involved in transitioning. In some cases, organisations do not have the administrative, technical and organisational skills required to implement MFA, and instead opt to either pay a third party to install it for them or abandon the idea all together. On average, it takes around 5-6 weeks for a full-time developer to build a minimum viable product for 2FA internally. Assuming a typical developer would cost around £1,750 per week, a basic fully functioning system would cost £10,500+ to produce. This price will increase if any of the work is outsourced and with any on-going maintenance and improvement costs.

Another way to install MFA is to use an application programming interface from a trusted 3rd party. Offloading the work to a trusted partner would increase financial costs but decrease time and organisational costs significantly, and would cause less disruption to day-to-day business.

Some users will inevitably become locked out of their accounts or forget their passwords, so maintained expertise is needed in the company to resolve any possible issues after the installation. This may involve employing someone full time to keep an eye on the security and daily IT issues in the company. These costs may be disconcerting to some, however, investing the time and money in becoming securer early on is vastly cheaper than the time, reputational and financial costs after a data breach.

According to MetaCompliance, the average cost of a data breach to organisations globally is £2.8 million per breach. Ensuring that employees make use of MFA may be tedious and somewhat difficult to coordinate, however the cost of implementing this is far lower than the risk of not installing MFA on company systems and experiencing a data breach. The reputational and financial damage after a data breach is enough to finish off many smaller companies who struggle to rebuild trust with consumers and keep themselves afloat while having to pay to amend their systems.

Useful resources

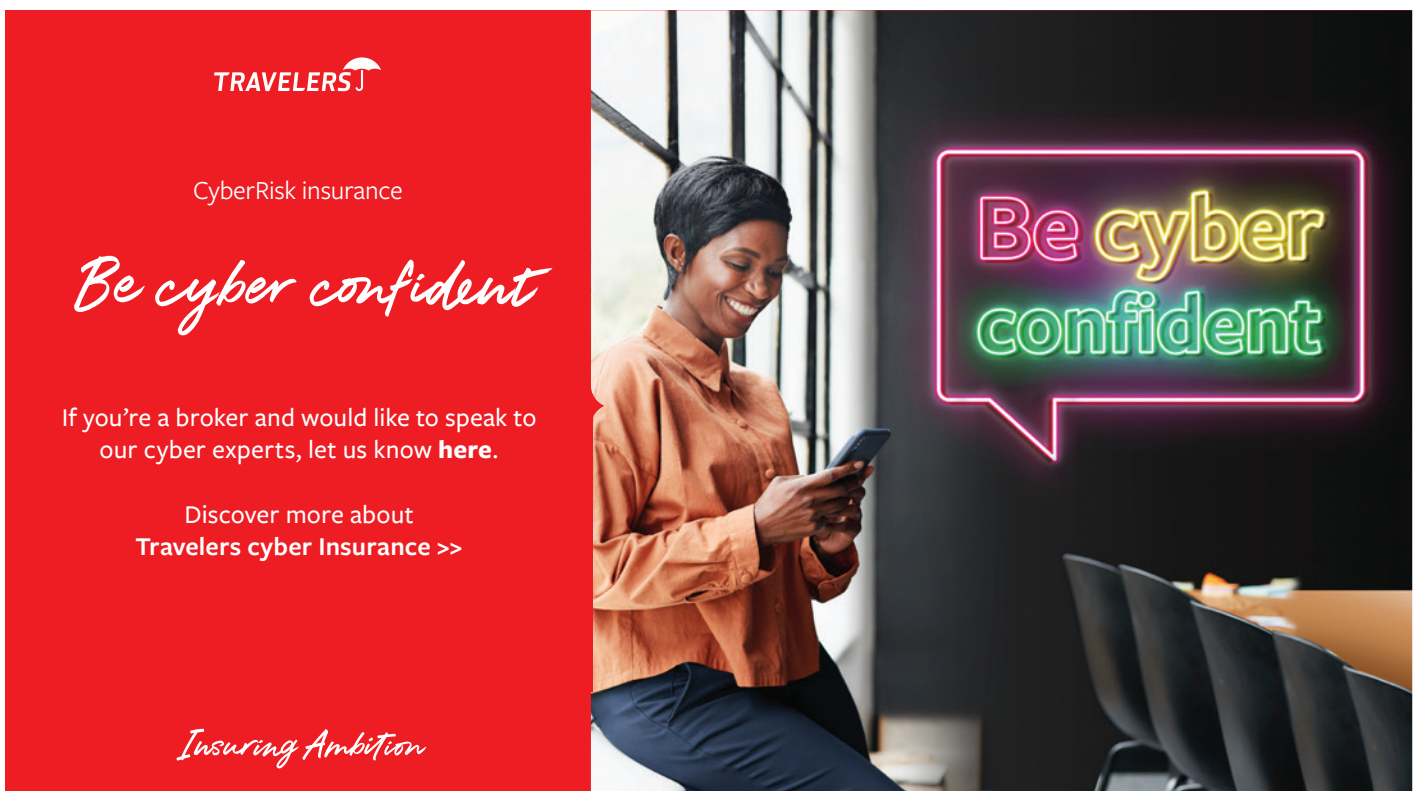
onelogin.com/learn/what-is-mfa

<https://messente.com/blog/most-recent/2fa-implementation-costs>

<https://docs.microsoft.com/en-us/security/compass/privileged-access-accounts>

<https://www.okta.com/identity-101/why-mfa-is-everywhere/>

<https://www.tripwire.com/state-of-security/security-data-protection/building-iam-benefits-sso-mfa-privileged-access-management/>



TRAVELERS

CyberRisk insurance

Be cyber confident

If you're a broker and would like to speak to our cyber experts, let us know **here**.

Discover more about
Travelers cyber Insurance >>

Insuring Ambition

Be cyber confident

About XCyber

Solve commercial problems with state-grade intelligence expertise. We are a bespoke cyber intelligence company with extensive experience in producing actionable intelligence for our clients. Our team are pioneers in cyber and the company draws its talent from former members of the UK's Public Sector, who bring with them many years of **outcome-driven, operational cyber experience** and specialised skills working across numerous Government departments and the UK's Intelligence and Security Agencies.

We focus on producing **intelligence-led, data-driven** and **evidence-based** reporting which enables decision making across our clients' varying needs. All our intelligence is delivered in qualitative, narrative format, providing actionable information that is easy to digest.

Our clients rely on our ability to do **scalable technical work**, translate that into human-readable analysis and actionable leads, all while maintaining a team culture that - in partnership with our clients - increases value through its **candour** and **integrity**.

Our modus operandum is to be a **strategic consultative partner**, led by a team of some of the most experienced professionals in cyber intelligence across the entire world. Together they have been working to develop and deliver effective solutions to some of the most **complex and challenging cyber** problems faced in both the public and private sectors.

Our current portfolio of client intelligence requirements includes the following thematic areas, across multiple geographic regions and sectors:

- Internal investigations (including insider threat), counter-intelligence, and specialist research (including counter terrorism, unlawful activism, and election integrity).
- Online reputation and defamation investigations, intellectual property and brand infringement (including counterfeiting and responding to disinformation campaigns).
- Countering cyber-enabled fraud and criminality (investigating and lawfully disabling the criminal ecosystems).
- Cyber risk and advisory at strategic, operational and tactical levels - including data protection, privacy and security.
- Supplier and supply-chain assurance, competitor analysis, crisis and breach response, red-teaming, and personal risk reports for executives.

To learn more about how **XCyber®** can support your business and clients, please contact our London, Mayfair office on the following address:

enquiries@xcybergroup.com

Our operational requirements team will be pleased to meet you.

xcyber®

THE HUMAN SIDE OF CYBER™

If you have found this useful and would like to receive these quarterly updates direct to your inbox please **[click here](#)** to register

The information provided in this document is for general information purposes only. It does not constitute legal or professional advice nor a recommendation to any individual or business of any product or service. Insurance coverage is governed by the actual terms and conditions of insurance as set out in the policy documentation and not by any of the information in this document.

TRAVELERS 

Travelers operates through several underwriting entities through the UK and across Europe. Please consult your policy documentation or visit the websites below for full information.

travelers.co.uk travelers.ie

TRV4360 09/21