July 2024

CYBER FOCUS

Gallagher Re

Multi-Factor Authentication:

Moving from ‘do you use it?’ to ‘how is it applied?’

Multi-factor authentication, or MFA, has become the star security control for securing online accounts in recent years, representing a crucial defence against a rising wave of attacks on cloud-based identities. However, this very success has also made MFA a prominent target for threat actors.

By adding an extra layer of authentication beyond passwords, a well-implemented MFA system can largely neutralize opportunistic attacks and significantly reduce the risks even from targeted attacks. Telecoms provider Verizon has reported[1] a significant reduction in breaches involving compromised credentials thanks to MFA, while Microsoft has said[2] it can block 99.9% of untargeted attacks.

Whilst MFA is undeniably a potent security tool, it can present insurers with a headache. External scans of policyholders' cybersecurity controls — while they play an important role in an underwriter's arsenal — can't reliably capture a policyholder's MFA configuration. In the absence of other 'inside the firewall' data, this leaves insurers dependent on self-attestation of MFA implementation in questionnaires.

And self-attestation is not infallible, as shown by the 2022 legal case involving International Control Services (ICS) and Travelers Property Casualty Company of America.[3] ICS claimed to have MFA in place, but a forensic investigation after a ransomware attack revealed it was absent.

Nevertheless, provided MFA procedures are in place and work as advertised, they are highly effective at deflecting untargeted attacks. Indeed, an estimated 86% of breaches involved the use of stolen passwords, showcasing the inherent weaknesses of single-factor authentication.[4] This has not gone unnoticed by threat actors.

Recent threat actor attention has focused on circumventing or undermining MFA security controls. Gallagher Re has observed this shift taking place in cyber insurance claims data. Our research suggests that fewer successful attacks and claims are correlated with traditional perimeter-based security controls, such as port security. Instead, cyber attackers are targeting the software and services used by an organisation, and more claims are resulting from credentials being leaked, or from breaches of the security protocols governing remote or mobile access to online services. This is where MFA's weaknesses come in.

There are various MFA bypass tactics available to cyber attackers, including:

MFA bypass tactics	Definition
SIM-swapping	A threat actor transfers a victim's phone number to their own SIM card, allowing them to intercept authentication codes.
MFA fatigue	An attacker bombards a victim with push notification requests, pressuring them into accepting one to make the noise stop.
Phishing	Fraudulent communications, such as emails or text messages, are intended to dupe employees into giving away their MFA credentials. Vishing, or voice-phishing, is a variant of the same technique involving fraudulent phone calls or messages.
Register a new device	Another variant of phishing, in which a threat actor tricks an IT administrator into enrolling a bogus device on the organisation's network.
Session hijacking	A threat actor takes over a valid user's session after they have been authenticated via MFA, thus bypassing it.

Some of these techniques have played a role in recent high-profile cyber attacks, as set out in the table below.[5,6,7]

Recent High-Profile Cyber Attacks

Twilio breach (2022)
Cloud communication company fell victim to a breach via SMS phishing

1. Phishing link via SMS message sent to Twilio employee
2. Login credentials and MFA codes captured by the threat actor
3. Threat gained legitimate access to Twilio's network

Uber breach (2022)
Transportation company fell victim to a breach using an MFA fatigue attack

1. Threat actor logged into the victim account, likely via compromised credentials
2. Threat actor bombarded the victim with MFA push notifications
3. Victim unknowingly provided the threat actor access to the account by accepting notification

MGM (2023)[8]
Hotel and Casino company fell victim to a ransomware attack instigated via phishing

1. Threat actor impersonated an employee to call the IT service desk
2. Service desk granted access to the user account
3. Threat actor gained admin rights within the MGM network

This increased activity by threat actors demonstrates some of the potential vulnerabilities of MFA procedures. However, these three case studies also show that these emerging attack methods are not insurmountable. For underwriters, this means shifting focus from the question'is MFA used?' to 'how is MFA implemented?'

The figure below highlights the susceptibility of different multifactor authentication technologies to various kinds of MFA bypass attacks. Understanding the relative exposures of different policyholders to these threat actor techniques enables more informed pricing and decision making.

MFA technologies' susceptibility to various forms of attack:

MFA technology	Susceptibility to...					
	SIM-swapping	MFA fatigue	Phishing	Vishing	Register a new device	Session hijacking
One-Time Passcode via SMS	High	Medium	Medium	Medium	Medium	Medium
Hardware tokens	Low	Low	Medium	Low	Low	Low
Biometric	Low	Low	Medium	Low	Low	Low
Authenticator app	Low	Medium	Medium	Medium	Low	Medium

This can be illustrated by comparing one older (but still widespread) form of multifactor authentication — SMS-based One-Time Passcodes — to the newer alternative of authenticator apps:

SMS-based OTP vs Authenticator app

Attack Type
SIM-swapping — an attack where a threat actor transfers a victim's phone number to their own SIM card, allowing them to intercept authentication codes.

HIGH

SMS-based OTP
One-time passcodes delivered via SMS have a **higher susceptibility** to SIM-swapping attacks. This is because a successful SIM-swapping attack allows a threat actor to intercept SMS-based OTPs.

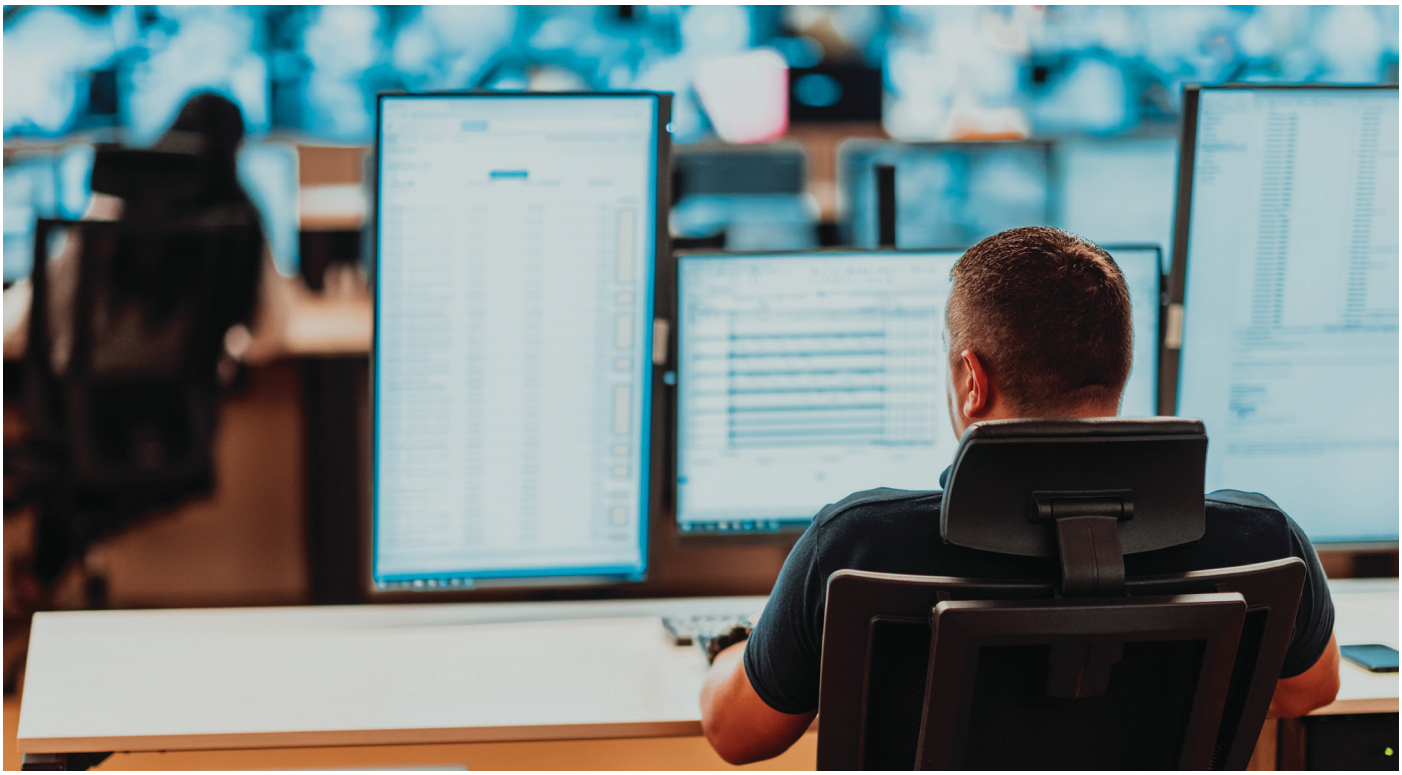
LOW

Authenticator app
Authenticator apps have a **low susceptibility** to SIM-swapping attacks. This is because the passcodes are generated within the app itself, rather than being sent via SMS. Therefore, a threat actor would be unable to intercept the codes.

MFA adoption within organisations continues to rise. However, insurers are increasingly aware of the nuances of implementation, and adopting a flexible approach.

For large businesses with complex IT environments and a high dependency on legacy systems, it can be difficult to universally apply strong MFA right across the organisation. However, compensating controls can be applied to limit increased exposure. For these companies, underwriters' questionnaires alone may not accurately reflect the actual state of MFA deployment across diverse systems, networks, and users.

Meanwhile, for the vast majority of smaller businesses, the effectiveness of MFA in stopping untargeted attacks in their tracks speaks for itself. Typically, insurers are not able to offer the same flexibility on control requirements here without risking upward pressure on loss experience. For SMEs, the broad message remains that even a simple MFA is better than no MFA at all.



Case Study: What is MFA Good Practice?

Implementation
Organisations must focus on properly implementing and enforcing MFA. This includes ensuring MFA is present on all login attempts, especially on high-value accounts such as administrator and service accounts, which are typically targeted by cyber threat actors.

Education
Ensuring employees are educated on best practices for MFA usage and up-to-date phishing techniques to help mitigate the risk of a successful MFA bypass attacks, which could lead to an account compromise.

Overall, MFA remains a crucial security control for securing accounts and identities, but it is not a silver bullet. Emerging MFA workaround techniques by attackers also serve as a pertinent reminder to cyber underwriting teams that constant adaptation of underwriting practices is needed to insulate portfolios from evolving threats.

Yet by understanding the details of how MFA is implemented across portfolios, insurers can make more informed decisions on the susceptibility of policyholders to emergent attack types. Insurance can also play an important role in educating policyholders by encouraging and sharing MFA best practices.

Authors:

Ed Pocock,
Global Head of Cyber Security

Dayan Patel,
Cyber Security Consultant

Gallaghe Re's Key Contacts:

Ian Newman,
Global Head of Cyber

Justyna Pikinska,
Global Head of Cyber Analytics

Sources:

[1] "2024 Data Breach Investigations Report." *Verizon*, accessed 16 May 2024, an estimated 86% of breaches involved the use of stolen passwords.

[2] Maynes, Melanie. "One simple action you can take to prevent 99.9 percent of attacks on your accounts." *Microsoft,* 20 Aug. 2019.

[3] https://www.americanbar.org/content/dam/aba/publications/litigation_committees/commercial/cases/2023/travelers-v-international-order.pdf

[4] https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf

[5] Ilascu, Ionut. "Okta one-time MFA passcodes exposed in Twilio cyberattack." *BleepingComputer*, 28 Aug. 2022.

[6] Badders, Tom. "The Uber Hack: MFA Fatigue is a Growing Threat to Enterprise Networks." *Telos*, 26 Oct. 2022.

[7] De Simone, Sergio. "Multi-Factor Authentication Fatigue Key Factor in Uber Breach." *InfoQ*, 24 Sept. 2022.

[8] Morrison, Sara. "The chaotic and cinematic MGM casino hack explained." *Vox*, 6 Oct. 2023.

Beyond Trust — "How Compromised Passwords Lead to Data Breaches & How to Prevent Them." *BeyondTrust,* 14 Dec. 2023.

Learn more about our client-focused, collaborative approach.
Connect with us today at **GallagherRe.com**.

It's the *way* we do it.

Gallagher Re