HYPR | THE IDENTITY ASSURANCE COMPANY

GUIDE TO CYBER INSURANCE AND MEETING MFA SECURITY REQUIREMENTS

The climbing costs and impact of cyberattacks makes cyber insurance critical for businesses in order to protect them against unacceptable cyber risk. Companies going to take out or renew policies, however, are finding that most cyber insurance carriers have instituted strict multi-factor authentication requirements in order to reduce premiums or even obtain coverage at all.

Why Is Cyber Insurance Needed?

Cyber insurance covers a business's liability in the event of a data breach or other cyber incident. Since general liability insurance does not cover cybersecurity claims, cyber insurance is necessary either as an endorsement or as a separate policy. For example, Colonial Pipeline was able to file a cyber insurance claim for the $4.4 million dollar ransom it paid to its attackers.[1]

The relentless attacks on organizations of all sizes have highlighted the necessity for cyber insurance for every organization, from small to large. According to Fitch Ratings, it's now the fastest growing insurance segment in the U.S.

Types of Cyber Insurance

While policies differ, the four basic types of cyber insurance include:

- **Privacy:** Insures against misused or stolen customer or organizational information. It can include coverage against class action suits and compliance violations such as GDPR, CCPA etc.
- **Security risk:** Sometimes referred to as network security risk covers the business in the case of a network failure. This can be due to ransomware, malware and other attack forms.
- **Operational risk:** The losses that refer to damages to the operating capability of an organization. This includes a loss of manufacturing output, service availability and service data.
- **Service risk:** This can be included together with operational risk or may be separated. This is the failure to provide a service due to a security incident.

Availability, Cost and Coverage

Policy premiums can vary greatly based on the size of the organization, coverage required and risk factors such as type of business, digital footprint and most importantly, security countermeasures the organization has in place.

The scope and damage of the Colonial Pipeline attack, the Solar Winds hack and other recent attacks, have resulted in massive payouts for cyber insurers.[2] In particular, the uptick in ransomware attacks created high loss ratios for carriers. As a consequence, premiums continue to skyrocket — up 110% in the first quarter of 2022 alone.[3] It's also increasingly difficult to even obtain cyber insurance.

Most cyber insurance underwriters mandate that specific security controls be in place in order to qualify for a policy. These may include a firewall, antivirus/EDR software, employee training, backups at an offsite facility and other elements such as secure account provisioning. Nearly all cyber insurance providers now also require companies to implement multi-factor authentication (MFA) or face premium penalties, sublimits, coverage exclusions or even denial of policies.[4]

What is Multi-Factor Authentication?

MFA requires two or more verification methods for users to gain access to a system, device, or application. In its most basic form, this consists of the familiar password plus one of these additional verification methods:

- **Knowledge:** Something you know, such as the answer to a security question, a PIN, or a one-time password.
- **Possession:** Something you have like a smartphone or hardware OTP token.
- **Inherence:** Something you are, which is biometric data like a fingerprint, face or voice.

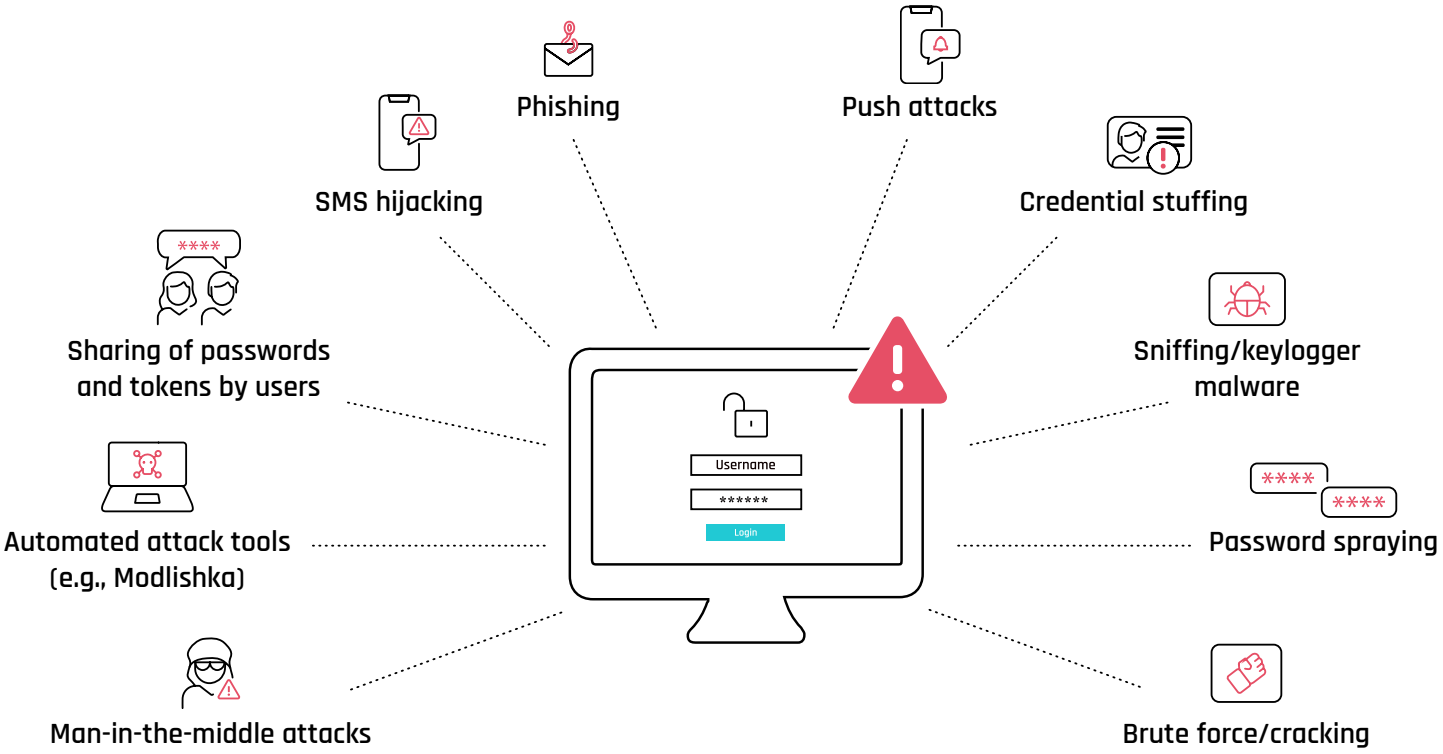
Cyber Insurance and MFA

Multi-factor authentication ranks high on the list of considerations for insurers. Credentials are the top entry vector for ransomware and, in fact, most attacks can be traced back to an issue with passwords or other authentication vulnerabilities. The 2022 Verizon DBIR report found that 82% of breaches involved the human element including the use of stolen credentials, phishing, misuse, or simply an error.

This statistic is not surprising given that most authentication schemes are still based on passwords. Additional security layers such as PINs, SMS links and OTPs really just introduce friction for the user and needless cost to the organization since they can be readily defeated by . attacks such as man-in-the-middle, credential stuffing, social engineering and push attacks.

Top 10 Authentication Security Risks

Attackers use multiple methods to bypass passwords and traditional MFA. These are the most common threats to guard against.



Obstacles to MFA

Security experts and cyber insurers have been recommending multi-factor authentication for years. So why haven't more companies already deployed it? In a recent survey, 49% of IT and security experts named poor user experience as a primary challenge in deploying traditional MFA solutions and 48% said they are difficult to integrate with current systems.[5] Workers and customers often resist MFA adoption as it requires multiple steps to authenticate.

The productivity hit that comes from traditional MFA also makes many organizations hesitate. Requiring employees to use an additional factor means it takes longer for them to get into the applications and systems they need to do their work. In the event of access issues, there is downtime and help desk drain until it can be resolved.

Of course cost also plays a role. Besides the deployment, management and help desk costs, there may also be hardware costs, such as security keys.

Perhaps the biggest blocker though comes down to the fact that traditional MFA just does not reduce risk enough. Security analysts have shown that 90% of MFA can be bypassed by phishing and other techniques.[6]

Passwordless MFA

This is where phishing-resistant passwordless MFA technologies come in. Login is fast and easy and, depending on the type of passwordless solution deployed, there may not be hardware costs beyond the smartphones your users already own. Most importantly, truly passwordless technology — where neither the user or service provider possess a shared or shareable secret — is far less vulnerable to attack.

That last point is important. Many solutions call themselves passwordless but they may simply hide a password, for example using biometrics to unlock a password. Or they may store credentials in a central database, which means they can be breached and stolen. Many cyber insurers specifically require phishing-resistant MFA as defined by NIST and the OMB.

Secure Desktop Authentication

An increasing number of cyber insurers specifically require MFA at the desktop. The majority of MFA solutions — both traditional and passwordless — cover application login only, or address limited desktop use cases. For example, they may not support all of your operating systems or remote desktop access.

When considering solutions, look for complete coverage from desktop to cloud.

Ten Passwordless MFA Solution Requirements

Keep this checklist on-hand when evaluating passwordless MFA solutions for your business.

Passwordless MFA Requirements	Meets Requirement?
Architecture complies with Zero Trust framework	☐
Authentication should be able to integrate with all the major identity providers (Okta, Ping Identity, Azure AD, etc.) so that you are not locked in to a specific IdP	☐
FIDO2 Certification end-to-end (not "FIDO like" or just for an element of the solution)	☐
Integration capabilities with SSO	☐
No passwords or shared secrets on the front end or back end	☐
Offline mode capabilities that do not fall back to shared secrets for when connectivity is not available	☐
Passwordless MFA for desktop login as well as native and cloud apps	☐
Trusted Platform Module (TPM) to store private keys	☐
Fast, single-gesture, user-initiated login	☐
Support for remote access including VDIs, VPNs and RDP	☐

Note: These are key buying criteria that should be considered in a passwordless MFA solution. This is not an exhaustive list. For a full list, please contact your HYPR representative.

Secured and Insured With HYPR Passwordless MFA

HYPR's True Passwordless™ MFA platform delivers uncompromising security coupled with a seamless user experience that will make your security department, end-users and your insurance carrier all happy. HYPR provides phishing-resistant login that scales from the desktop to the cloud. It uses a combination of private and public key encryption, so that, in essence, the user becomes the authentication mechanism rather than a password, or device. This type of frictionless phishing-resistant MFA conforms to the FIDO standard which is recognized by the CISA as the gold standard for Zero Trust Authentication.

HYPR partners with cyber insurance carriers in order to offer their customers a Passwordless MFA solution that meets and exceeds the carrier's requirements to qualify for cyber insurance. We also work with organizations directly to quickly and easily deploy passwordless MFA that helps them realize additional benefits including:

- **Lower risk** by changing the economics of attack and reducing the likelihood of a breach. For example, HYPR clients have achieved a 98.4% reduction in account takeover, and zero phishing incidents.
- **Improve user satisfaction** with a frictionless authentication experience. For example, users of HYPR spend **300% less time** authenticating than with traditional authentication approaches.
- **Lower TCO** of authentication deployment and administration. For example, HYPR customers have experienced **35% fewer helpdesk calls**, and as much as **$2.4 M savings** in incident response costs.
- **Quickly meet many of the regulatory compliance standards** necessary such as GLBA, SOX, HIPAA, SOC and more.

Sources:

1 https://www.wired.com/story/ransomware-insurance-payments/
2 https://www.crn.com/news/security/solarwinds-hack-could-cost-cyber-insurance-firms-90-million
3 Marsh Global Insurance Market Index Q1 2022, Marsh LLC, 2022
4 U.S. Cyber Market Outlook, Risk Placement Services, Inc., 2021
5 The State of Passwordless Security 2022, HYPR, 2022
6 Hacking Multifactor Authentication, Roger Grimes, Wiley, Sept. 2020 https://www.cisa.gov/uscert/ncas/tips/ST04-023 https://pages.nist.gov/800-63-3-Implementation-Resources/63B/Verifier/

See how passwordless MFA can secure your workforce and customers.

Visit: hypr.com/demo

About HYPR

HYPR creates trust in the identity lifecycle. HYPR Identity Assurance provides the strongest end-to-end identity security for your workforce and customers, combining phishing-resistant passwordless authentication with adaptive risk mitigation, automated identity verification and a simple, intuitive user experience. HYPR has a demonstrated track record securing organizations globally, with deployments in some of the most complex and demanding environments, including 2 of the 4 largest US banks, manufacturers, leading critical infrastructure companies and other technology-forward businesses. HYPR's solutions have been independently validated to return a 324% ROI.