Cybercrime incidents have been on a rise since last decade. The Colonial Pipeline attack, one of the most impactful cyber incidents of the decade was a result of a single password being compromised. The ever-growing rate of cybercrime has pushed institutions and organizations across the world to rethink their IT infrastructure and find some good authentication measures to verify end-user identity.

Earlier this year, the US President, Joe Biden signed an Executive Order on improving nation's Cybersecurity. The order mandates Multi-Factor Authentication (MFA) for all federal agencies in the United States. This sent a soft signal to all cybersecurity insurance companies that still leave MFA out of their list of requirements for cyber insurance. As a result, cybersecurity insurance providers mandated that MFA must be in place as a base requirement to get coverage from a cyberattack.

While cyberattacks are on a rise, cybersecurity insurers are ensuring that their payers should have minimum security requirements in place to prevent a successful attack.

Cyber Insurance – What is it?

A cybersecurity insurance, also called cyber liability insurance is a coverage against financial losses caused by cyber incidents (such as data breaches) and offers technical and recovery support. Cyber insurance companies require their customers to adopt minimal preventive measures to be eligible for insurance coverage. Every cyber insurance policy might have its unique set of criteria, but most of the companies are now requiring MFA to have you covered.

What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication, or an MFA is an authentication measure that used at least two different authentication factors to verify user's identity. When an MFA is on and you login to an application, you will have to provide at least two proofs of your identity to gain access to the application. Apart

from a username and a password, the system asks you additional proofs of your identity, such as security questions, SMS code, Email OTP, Mobile Push, or Biometrics.

The Benefits of MFA

MFA is your golden armor, a key to defense against the threat of compromised passwords. 2021 Verizon Data Breach Investigation Report (DBIR) found that credentials are the #1 data type stolen and hacked credentials resulted in 61% of all breaches.

Obviously, when an attacker is using a valid set of credentials, why would your firewall, antivirus, or other technologies you might be using will flag anything unusual? Your systems will assume that the users accessing your network are who they say they are.

Adding a multi-factor security will protect your users' account with:

- **Something you know** – A knowledge factor such as password
- **Something you have** – A possession factor such as a security key or phone
- **Something you are** – An inherence factor such as biometrics

This means even if your password is stolen, the attackers won't be able to access your account without all the required factors.

Why Do Cyber Insurance Companies Want Their Customers to Deploy MFA?

Users have varying levels of accesses and privileges to wide range of applications in a company. The company data is hosted by different providers and communication happens in an open network. Access and privileges are based on user identities.

Attackers try to find vulnerability in the infrastructure of a company and use this puncture point to perform a security breach. Compromised accounts form the basis of most of the attacks. If you only protect user identities with passwords, you are inviting hackers to exploit your IT infrastructure.

MFA adds an additional layer of security to your IT infrastructure and prevents most of the security breaches that are a result of compromised credentials. It is not surprising that cybersecurity insurance companies demand their current and future customers to deploy MFA.

How QuickLaunch can help?

MFA is a vital layer of protection against business interruption and identity theft that can result from a cyberattack. QuickLaunch MFA is an easy-to-deploy, two-factor authentication solution that is affordable and provides that extra layer of security. You can verify end user identity through multiple authentication factors such as SMS, Email, Security Questions, Google Authenticator, Microsoft Authenticator, Mobile Push, and Biometrics.

QuickLaunch also offers Adaptive Authentication solution that adapts and presents the user with the appropriate level of authentication for the given level of risk to ensure eliminating low-risk activities inappropriately burdensome on the user or high-risk activities too easy to hack.

QuickLaunch has a proven track record of deploying Multi-Factor Authentication and Adaptive Authentication solutions in 3 weeks or less. Our clients leveraging QuickLaunch Multi-Factor Authentication or Adaptive Authentication solutions have significantly reduced their security risk and other report risk mediation by 79%!