U.S. Risk, LLC

MULTI-FACTOR AUTHENTICATION (MFA)

No matter how strong password credentials may be to secure an account, there are often equally strong attacks against them. When establishing appropriate access for users, it's important that users prove they actually are who they claim to be. MFA, or multi-factor authentication, is an authentication method that requires the user to provide two or more credentials in order to gain access to an account. In fact, MFA has become a common requirement from cyber underwriters in order to secure coverage and is a core component of a strong identity and access management policy.

GUARDING AGAINST ATTACKS

MFA helps protect against unauthorized access, data breaches and password-based cyber attacks. It serves as a second barrier by verifying something a user can know (such as asking for your mother's maiden name or where your first job was held), something a user has (such as a unique key, a cell phone with a code), or something a user is (such as facial recognition, fingerprint scan). If this second factor of authentication cannot be verified, then the account remains locked, and a potential attack is prevented.

EXPANDING MFA PROTECTION

One expansion of two-factor authentication is something called Risk-based Authentication, or Adaptive Authentication. This process analyzes additional factors by considering context and behavior when authenticating and often uses these values to assign a level of risk associated with the login attempt.
For example:
Location: From where is the user when trying to access information? Does it fit previous patterns?
Time: When you are trying to access company information? Is that time atypical?
Device: What kind of device is used? Is it the same one used yesterday?
Connection: Is the connection via private network or a public network?
The risk level is calculated based upon how these questions are answered and can be used to determine whether or not a user will be prompted for an additional authentication factor or whether or not they will even be allowed to log in.

TIPS TO PROTECT YOUR ORGANIZATION

Some 99.9% of account compromise attacks can be blocked by MFA. Some tips to help protect your organization include:

- Implementing a strong multifactor authentication solution, such as an app or hardware dongle.
- Checking that your cloud providers support strong authentication.
- Adding a PIN or passphrase to cell accounts to prevent criminals from swapping SIM cards using stolen information.
- Making sure you have cyber coverage in place to add another layer of protection.

Where Should MFA Be Implemented?

To thrive in the modern threat landscape, MFA needs to be expanded beyond just the most privileged accounts into all access to all systems. MFA is recommended to be implemented in these areas:

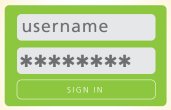
- Privileged user accounts
- Remote access to computer systems by employees
- Remote access to computer systems by vendors and independent contractors
- Remote access to email
- Cloud resources (Office 365 etc.)
- Remote Desktop Protocol (RDP) and virtual desktops
- To restrict access to your backups
- For any additional applications (internal or external) that contain personally identifiable information

Types of MFA Authentication Methods

MFA is successfully enabled when at least two of these categories of identification are required in order to successfully verify a user's identify prior to granting access.

INHERENCE
Fingerprints, voice or facial recognition

POSSESSION
A badge or cellphone



KNOWLEDGE
A password or personal pin

THE BOTTOM LINE

MFA is an important preventive measure to take to avoid security breaches, but it is not an all-encompassing solution to protect an organization. Even the most diligent management firm can be susceptible to a claim. A trusted insurance expert highly experienced in all the various forms of cyber liability and how to customize policy terms needs to be brought into the process as early as possible to ensure coverage for critical risks, future potential claims management, and the latest developments in terms and conditions.