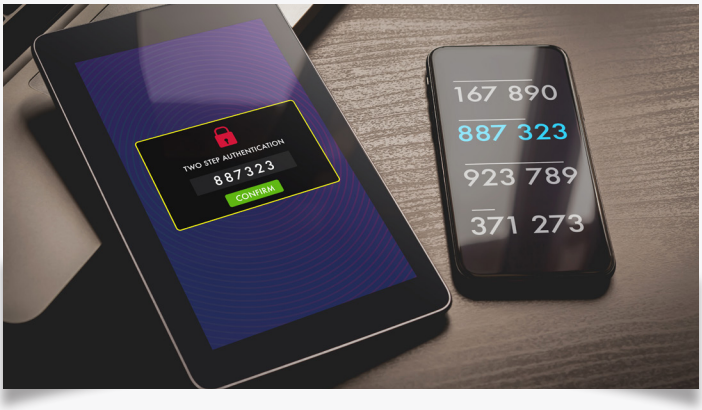
CRC Group
Wholesale & Specialty

Multi-Factor Authentication (MFA): A Must Have for Cyber Coverage

Over the last 18-24 months the rate of ransomware attacks has skyrocketed in both frequency and severity, driving significant changes in the cyber insurance marketplace. In years prior, cyber submissions were simple and it was easy to obtain bindable quotes from multiple markets. When it came to renewals, underwriting typically only required updates around major business changes. But, times have changed and these days underwriters across the board are asking for more information related to ransomware loss controls and IT risk management. It's now common practice to require that insureds have Multi-Factor Authentication (MFA) in place (especially when it comes to email access) before providing a quote for most accounts. Without MFA, clients risk non-renewal or a retention hike of 100% or more.



Microsoft records more than 300 million fraudulent cloud service sign-in attempts every day.[1]

WHAT IS MFA?

Multi-Factor Authentication is a cybersecurity measure that requires users to confirm multiple factors verifying their identity prior to accessing a network or system. Generally, users must provide a password, verify access by inputting a code sent to another device, or confirm access with biometric data such as a fingerprint.[2] Those hesitant to adopt MFA are often under the misconception that it requires the purchase of additional external hardware or are concerned about potential user disruption.[7] While it's true that MFA can require users to take an extra step or two at login, it's not complicated and doesn't always require buying new hardware.

WHAT SHOULD BE PROTECTED WITH MFA?

MFA should be used to protect remote network and email access as well as administrative access. This prevents system intruders from breaching networks to deploy ransomware, erase valuable data, or steal sensitive information for malicious purposes through a variety of commonly successful cyberattacks such as phishing or keylogging.[7]

MFA Protects Against[7]

- Phishing / Spear Phishing Attacks
- Keyloggers
- Credential Stuffing
- Brute Force Attacks
- Reverse Brute Force Attacks
- Man-in-the-Middle (MITM) Attacks[7]

HOW DOES MFA PROTECT INSUREDS?

Brokers are seeing ransomware or social engineering claims hit almost weekly. Such claims can cost hundreds of thousands of dollars and require pricey forensic investigations that take several weeks to complete. Such attacks often start with compromised passwords or login IDs. These credentials can be the weakest point of a company's digital footprint because employees often use the same password for multiple systems, create passwords that are too simple, share credentials with others, or inadvertently give information to cyber criminals.[1]

MFA protects businesses by adding a layer of security that can block 99.9% of attacks stemming from compromised accounts. For example, a phishing attack may obtain a user's credentials, but be unable to provide the fingerprint or security question response required for authentication.[1] Because every attack begins at an endpoint, companies should also be utilizing Endpoint Detection and Response (EDR), in collaboration with MFA, to maintain visibility into all endpoints. Employing MFA and EDR together will significantly minimize the threat of a breach, especially when combined with mature patching requirements, employee training, and increased awareness.

Cybersecurity Best Practices

- Utilize MFA for remote network/ email and administrative access
- Employ EDR to monitor all endpoints
- Use segregated/ air-gapped backups
- Test off-site or cloud backups routinely

31% of all targeted cyberattacks are aimed at businesses with fewer than 250 employees.[3]

HOW CAN CLIENTS IMPLEMENT MFA?

Clients can choose from a variety of vendors to employ MFA and EDR. Most companies already paying for products like Microsoft Office 365 or Salesforce can obtain MFA services from those providers. There are also several commonly known companies that offer comprehensive services at reasonable prices. There are easy-to-deploy, two-factor authentication solutions that can cost as little as $3 per user, per month. The cost of implementing MFA can vary and ultimately depends on the type of solution chosen as well as the business's requirements, including the number of systems and accounts protected by MFA.[6]

Common MFA Providers*

- Duo
- Okta
- LastPass
- OneLogin
- Auth0

Common EDR Providers*

- Carbon Black Cloud
- Crowdstrike Falcon Insight
- SentinelOne
- Windows Defender Endpoint

BOTTOM LINE

MFA is a vital layer of protection against first party losses and business interruption that can result from a cyberattack. While the economic turmoil of the last year impacted companies of all sizes, the hit taken by many mid-sized companies and small businesses can make it tempting to skip improving cybersecurity or buying cyber insurance. However, CNBC recently reported that only 14% of small businesses have the means to defend against cyberattacks, and 60% of companies that suffer a cyberattack close their doors within 6 months due to an inability to recover.[4]

Agents and insureds would be wise to take a proactive stance toward obtaining coverage, and begin remarketing accounts 2-3 months prior to renewal, keeping in mind that there are many products available and multiple ways to purchase coverage. CRC Group now leverages Cyberwrite technology on the REDY platform to generate customized insights into clients' cybersecurity and the likely cost of a claim. Leaning on the expertise of CRC's team throughout the quoting and buying process can ensure that your clients receive optimal coverage for the best possible price. Contact your CRC Group producer today to discover how we can help protect your clients in today's digital environment.

Contributors

- Darren Valencia is a Vice President located with CRC's Nashville office, an active member of the ExecPro Practice Group, and a member of the Cyber Specialty Team.
- Mark Smith is a Senior Vice President with CRC's Seattle office. He's an active member of the ExecPro Practice Group and a member of the Cyber Specialty Team.

ENDNOTES

1. One Simple Action You Can Take to Prevent 99.9 Percent of Attacks on Your Accounts, Microsoft, August 20, 2019. https://www.microsoft.com/security/blog/2019/08/20/one-simple-action-you-can-take-to-prevent-99-9-percent-of-account-attacks/
2. What is Multi-Factor Authentication? Cisco. https://www.cisco.com/c/en/us/products/security/what-is-multi-factor-authentication.html#~how-mfa-works
3. 8 Reasons You Should Turn to Multi-Factor Authentication, TechBeacon, https://techbeacon.com/security/8-reasons-you-should-turn-multi-factor-authentication
4. How Cybercrime Impacts Organizations and What You Can Do About It, Legal Reader, February 21, 2020. https://www.legalreader.com/how-cybercrime-impacts-organizations/
5. Hackers Attack Every 39 Seconds, Security Magazine, February 10, 2017. https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds
6. Multi-Factor Authentication for Small Business, Totem, September 10, 2020. https://www.totem.tech/multi-factor-authentication/
7. What Type of Attacks Does Multi-Factor Authentication Prevent?, Onelogin, 2021. https://www.onelogin.com/learn/mfa-types-of-cyber-attacks

*CRC Group does not endorse any specific company or provider; the names listed in this article are simply informational references, organizations are responsible for research and selecting MFA and EDM services based on business needs.