WHA WISCONSIN HOSPITAL ASSOCIATION
ADVOCATE. ADVANCE. LEAD.
The Valued Voice

Vol. 68, Issue 42 Thursday, October 17, 2024

Guest Column: Two Steps Ahead: Why MFA is Essential

By Alex Friedl, M3 Insurance - WHA's Premier Partner


Alex Friedl

You wouldn't leave your office unlocked overnight or hand out keys to just anyone, right? When it comes to securing your business, physical protection is a no-brainer. But what about your digital doors? In today's tech-driven world, cyber threats are as real as a break-in, and locking down your sensitive data requires more than just a strong password. That's where **multifactor authentication (MFA)** steps in—an essential digital security measure that ensures only the right people have access to your critical business systems. Just like bolting the door, MFA helps keep cybercriminals out of your network, adding an extra layer of defense where it's needed most.

MFA is a means of providing access with two pieces of evidence to confirm your identity. One factor is your username and password, also called your login credentials. Multifactor authentication introduces a second factor such as a text message, biometric information, or a login push from an authenticator application.

MFA is widely regarded as a critical cybersecurity measure—and for good reason. Imagine you're working remotely and need to access your company's network via a **virtual private network (VPN)**. While the VPN offers the convenience of working from anywhere, it also opens the door for cybercriminals to potentially do the same. Without MFA, all a hacker needs to breach your network is your login credentials. By adding a second layer of verification, MFA creates an additional obstacle, making it far more difficult for unauthorized users to gain access to your system.

In fact, insurance carriers view multifactor authentication as a critical security control and in most cases, it is a prerequisite to qualify for insurance. In particular, insurance carriers like to see multifactor authentication in place for email access, remote access to your network, and for all administrative accounts. Some insurance carriers also prefer MFA be implemented in additional areas, such as accessing backups and critical software systems. Without MFA, you risk being denied coverage or facing reduced protection for specific losses, like ransomware attacks.

Implementing multifactor authentication (MFA) is crucial for securing your business, but it's equally important for personal accounts, especially those tied to finances or sensitive information. Enabling MFA on online banking accounts, 401Ks, IRAs, and other investments adds an extra layer of protection against unauthorized access. Fortunately, most major financial institutions offer MFA as a standard security feature, making it easier to safeguard your personal assets.

Key Takeaways
MFA is an important security measure that should be implemented both within your business and on your personal accounts. Though entering a second authentication factor may feel like a minor inconvenience, this simple step can be the difference between preventing a ransomware attack on your business or stopping a thief from draining your personal bank account.

Reach out to your **M3 Client Executive** to discuss your current protection for your organization and to learn more about cybersecurity risk management.

Other Articles in this Issue

- Hurricane's Impact Continues to Constrain IV Fluid Supply Chain
- Registration Now Open for the 2025 WHA Health Care Leadership Academy
- Five Wisconsin Rural Hospital Leaders Recognized as "CEOs To Know" by Becker's
- Guest Column: Two Steps Ahead: Why MFA is Essential