Expanding Your Cyber Protection: New Tools Now Available Through SVMIC

By Rana McSpadden, FACMPE

This year, SVMIC transitioned our cyber liability carrier from Tokio Marine to Beazley Cyber Insurance. With this change, policyholders now have access to an expanded suite of resources in addition to those already offered by SVMIC. Throughout the year, several of these new tools and services will be highlighted.

To begin exploring these resources, visit the Cybersecurity Resource Access page through the Vantage account portal. This page provides an access link and step-by-step instructions for creating an Admin account. The link will direct users to the Breach Solutions portal, where the account setup process is completed. Once the Admin account is active, staff email addresses can be added, and resources, such as educational modules or risk assessments, can be assigned. Email addresses may be added individually or uploaded in bulk using a comma separated values (CSV) file. After staff email addresses are uploaded and assignments are made, each staff member will receive an email directing

them to the Breach Solutions portal, where they can create their individual staff account to access assigned tools. It is recommended that staff be notified in advance, so they know to expect this email.

An effective cybersecurity program begins with identifying gaps in your staff's knowledge and awareness of secure digital practices. Uncovering these gaps is essential for reducing vulnerabilities that can lead to data breaches, reputational harm, or HIPAA compliance issues. One of the first tools administrators may want to assign is The Risk Assessment tool. It evaluates each staff member's understanding and everyday use of secure cyber practices such as two-factor authentication and strong password design. Once completed, staff receive an individualized score along with practical recommendations to strengthen their cybersecurity habits. Administrators gain a consolidated view of staff performance, making it easier to identify trends, tailor future training, and make data-driven decisions about additional education that may be needed. Taking advantage of this information not only supports immediate improvement but also helps cultivate a long-term culture of cybersecurity awareness.

Access to these expanded cybersecurity resources offers practices a valuable opportunity to strengthen their overall security and better protect sensitive information. Integrating these tools into routine operations encourages consistent, informed digital behaviors across the workforce. SVMIC remains committed to providing the support and guidance needed to navigate the evolving landscape of cyber risk with confidence.

If you have questions about HIPAA, cybersecurity, or access to SVMIC resources, call 800-342-2239 or email Contact@svmic.com.

If you experience a cybersecurity or other HIPAA related incident, contact SVMIC as soon as possible by calling 800-342-2239 and ask to speak with the Claims department.

Other individuals in your organization may benefit from these articles and resources, such as your administrator, privacy or security officer, or information technology professional. They can sign up for a Vantage account here.