Multi-Factor Authentication Requirements on the RPSSmallBusiness.com Platform – Here is What You Need to Know

In today's rapidly changing cyber insurance market, insurance companies are increasingly asking in-depth questions about how organizations are protecting themselves from cyber threats, particularly with respect to ransomware prevention. This barrage of new acronyms can be daunting for those less familiar with information security policies and procedures. Here, we take a quick look at Multi-Factor Authentication, as MFA will have an impact on insureds in the RPSSmallBusiness.com portal.

Multi-Factor Authentication (MFA)[i]

MFA, sometimes referred to as two-factor authentication or 2FA, is a security enhancement that allows you to present two pieces of evidence – your credentials – when logging in to an account. Your credentials fall into any of these three categories: something you know (like a password or PIN), something you have (like a smart card), or something you are (like your fingerprint). Your credentials must come from two different categories to enhance security – so entering two different passwords would not be considered multi-factor.

Research from both Microsoft and Google suggests that MFA can block over 99% of account compromise attacks. However, reports suggest that only 57% of global businesses are using MFA. The May, 2021 Colonial Pipeline ransomware attack was reported to have occurred from a hack of an inactive Virtual Private Network (VPN) that did not use MFA. Vendors in the MFA space are making the process easier, less expensive and more flexible for businesses of all sizes to implement and users to access. MFA is not only easy and cost-effective to deploy, but intuitive and user-friendly for all employees, regardless of technical savvy.

What should be protected with MFA?

- Remote Network Access
- Privileged/Administrative Access
- Remote Access to Email

Essentially, any and all remote access to sensitive information should be protected via Multi-Factor Authentication. For MFA to be fully effective, protection should extend to all employees, regardless of role.

If insurers are requiring MFA, where can organizations get it and how much does it cost?

Often times, implementing MFA for an organization is free, depending on which vendors are used for which applications (for instance, Gmail, Outlook and others). For 3rd party applications, implementing MFA can be easy and cost-effective. Examples of MFA vendors, complete with 3rd party ratings and contact information, can be found here and here. The average cost to implement MFA can vary between free (if already included in the software configuration you have purchased), or generally between $3.00 and $9.00 on a per-user/per-month basis.

Risk Placement Services is not qualified to provide legal or information security related technical advice. As such, we cannot endorse vendors for MFA implementation or consultation. Sample vendors are provided herein as examples only. We recommend that insureds also consult with their existing IT vendors for advice on implementation, as capabilities such as these are often available through current IT configurations, often times at no additional cost. This material is for general informational purposes only. It is not intended as, nor does it constitute legal or professional advice, nor is it an endorsement of any source cited or information provided. This information does not amend, or otherwise affect, the terms, conditions or coverages of any insurance policy placed by Risk Placement Services, Inc.

[i] **Source: National Institute of Standards and Technology (NIST) Back to basics: Multi-factor authentication (MFA) | NIST**