CSBS

MULTI-FACTOR AUTHENTICATION (MFA): QUESTIONS BOARD MEMBERS SHOULD ASK

Below are some questions you may ask management to ensure MFA has been appropriately implemented to protect against cyber threats.

1. **Has multi-factor authentication (MFA) been implemented in the institution? If so, does the institution rely on stronger application-based or phishing-resistant authentication methods (FIDO or public key infrastructure), as opposed to weaker SMS (text) or voice-based authentication?**

   WHY THIS IS IMPORTANT: MFA is a foundational security control that provides an enhanced means of verifying the identity of a system user by requiring the user to provide two or more authentication factors (i.e., something you know, something you have, or something you are) at login. While the use of <u>any</u> form of MFA is preferable to using none, it is important to understand that there are multiple methods of implementing MFA, as well as variations in the degree of security provided by each MFA type. In short, <u>all MFA is not the same</u>.

   - *SMS (text) and voice-based MFA methods are common but are the <u>weakest</u> form of authentication and, according to CISA, should ideally be used only as a temporary solution until stronger methods can be implemented in the institution.*
   - *Stronger authentication methods include authentication via mobile push notification (with or without number matching); one-time passwords; and token-based one-time passwords.*
   - *"Phishing-resistant" forms of MFA such as <u>FIDO</u> or <u>WebAuthn authentication</u> and <u>public key infrastructure (PKI)</u> authentication implementations are the <u>gold standard</u> for authentication and can generally offer superior protections against phishing, "push bombing", and other threats.*

2. **How has MFA been implemented?**
   - ☐ **For privileged access management (PAM) (domain administrative access, application administrative access, etc.)**
   - ☐ **For all users that access any cloud-based service (mortgage origination, HR platforms, etc.)**
   - ☐ **For cloud email services, such as Microsoft 365 and others**
   - ☐ **For access to external applications hosting non-public information (NPI)**
   - ☐ **For VPN/Remote Desktop (RDP) access into the network**
   - ☐ **For vendor access into the network**
   - ☐ **For internal service accounts**
   - ☐ **For customers accessing NPI (e-Banking services, remote deposit capture, etc.)?**

   WHY THIS IS IMPORTANT: MFA is implemented within an organization with a goal of strengthening authentication for critical systems and data, as well as protecting the institution against the use of stolen or "guessed" credentials. <u>CISA</u> recommends an organization-wide approach when implementing MFA as it is more effective to implement MFA across all systems and applications

instead of implementing redundant, isolated solutions for individual applications. Further, it is important for management to identify systems in which MFA is not supported and develop plans for upgrading these systems or migrating to new systems where MFA is supported. For organizations who elect to forego an immediate enterprise-wide implementation of MFA, the critical areas of focus for implementation of MFA typically include [privileged access management, email and other cloud-based services, applications that host nonpublic information, and remote access (including any vendor access) into the network, among others](.).

3. ***Does the institution have a plan for future implementation of MFA to protect critical functions and data for areas where it is <u>not</u> currently implemented?***

    <u>WHY THIS IS IMPORTANT</u>: As previously mentioned, CISA recommends taking an organization-wide approach to the implementation of MFA. However, there are a number of factors, such as financial and operational concerns, that can limit an institution's ability to immediately implement an enterprise-wide solution. In these instances, an institution would be well served to carefully evaluate risk and prioritize areas, such as those mentioned above, where MFA implementation is warranted. Due to the potential financial and operational impacts of implementing an MFA solution, it is also advisable that the institution appropriately plan for implementation throughout critical areas via budgeting and strategic planning efforts.

4. ***Are MFA applications properly configured, monitored, and supported by other security mechanisms to afford expected protection?***

    *<u>WHY THIS IS IMPORTANT</u>: MFA is <u>not</u> a "magic bullet", nor a substitute for other security controls when sensitive information is being protected. [Recent FFIEC guidance on authentication](.) states that, "When a financial institution management's risk assessment indicates that single-factor authentication with layered security is inadequate, MFA or controls of equivalent strength as part of **layered security** can more effectively mitigate risks." When MFA is implemented, it is important that the chosen technology is **configured properly, monitored, and supported by other necessary security mechanisms as part of a layered security approach**. Misconfigured or improperly managed MFA applications can provide a false sense of security to the institution and may create unintended weaknesses that may be easily exploited by cyber threat actors.*