Strengthening user access security checklist

Don't wait to be a victim of cybercrime before you implement MFA. It is a crucial control that is often found to be missing, which can lead to being a key contributing factor to successful cyber-attacks and fraudulent activity.

This high-level checklist, which is part of the comprehensive QBE MFA Guide can be used as a guide to ensure critical controls for strengthening user access security for your business are implemented. You may wish to create more detailed checklists for the individual steps that may be required to achieve each of these actions for your business. Should you have any comments, please add them below by clicking on the text fields provided.

Action checklist

1 Undertake a cyber resilience risk assessment to identify the critical assets, functions and all the access points to where sensitive data resides; and the MFA/user access control status for each of these. ☐

Add a comment

2 Ensure the procurement process requires service providers to have minimum security standards, including MFA capabilities; and ensuring their systems are effectively protected. ☐

3 Schedule regular reviews to ensure MFA is working effectively across the business, and new exposures have been sufficiently protected. ☐

4 Ensure your organisation's password policy offers guidance on using strong, unique passwords for each access point or account. ☐

Action checklist, continued

5 Consider the use of password managers which can generate random strong passwords for users. Train your staff on how to make the best use of password managers. ☐

6 Use risk-based policies to establish which triggers should alert relevant users, administrators, or management. e.g., where unauthorised access has been detected. ☐

7 Ensure there is an established process to change passwords or replace MFA methods promptly if a user knows or suspects the password, other authentication method or account has been compromised. ☐

8 Establish a clear and accessible reporting process, which staff and/or stakeholders are regularly made aware of, and encouraged to utilise. ☐

9 Build and maintain a culture within your business where staff and stakeholders feel confident to speak up, especially in relation to security concerns or potential incidents. ☐

10 Educate staff and customers to remain vigilant to social engineering scams and refrain from revealing any personal or security information. ☐

For support with the above key actions, check out the QBE MFA Guide and the Useful Links within it. Many of the useful links are from the NCSC website, which is regularly updated, and the guidance is generally globally applicable – so worth reviewing.

QBE European Operations
30 Fenchurch Street
London EC3M 3BD
tel +44 (0)20 7105 4000
QBEeurope.com

443204/2209