Markel Cyber 360[SM]

Section D: Network Security contd. (Ransomware Supplement)

1. Do you authenticate emails using: ☐ SPF, ☐ DKIM and/or ☐ DMARC

2. Do you use O365 in your organisation?
   - ☐ Yes. Have the following been implemented: ☐ MFA, ☐ ATP, ☐ Macros disabled by default
   - ☐ No. Which product do you use for email monitoring (e.g. Proofpoint) Click or tap here to enter text.

3. Do you allow local admin rights on workstations? ☐ Yes ☐ No

4. Do administrative/privileged accounts use a privilege access management (PAM) tool (e.g. CyberArk)?
   ☐ Yes ☐ No. Which product(s) do you use: Click or tap here to enter text.

5. Do you use an endpoint protection (EPP) product? If so, which product(s): Click or tap here to enter text.

6. Have you deployed an endpoint detection and response (EDR) tool that covers 100% of:
   ☐ Servers and ☐ Endpoints? If so:
   - Which product(s): Click or tap here to enter text.
   - If the EDR tool offers AI/automated rules based enforcement, has this been enabled?
     ☐ Yes ☐ No ☐ N/A

7. Does all remote access to your network and corporate email require multifactor authentication (MFA)?
   ☐ Yes ☐ No

8. Have you disabled remote desktop protocol (RDP)? ☐ Yes ☐ No
   - If No, have you implemented the following: ☐ VPN ☐ MFA ☐ RDP Honeypots

9. Do you operate a SIEM monitored 24/7/365 by an internal SOC or MSSP? ☐ Yes ☐ No

10. Does your incident response plan (IRP) specifically address ransomware scenarios? ☐ Yes ☐ No

11. How frequently do you back up critical data? ☐ Daily ☐ Weekly ☐ Monthly ☐ Other

12. Do you keep a copy of your critical backups offline and inaccessible from your network? ☐ Yes ☐ No

13. Which of the following are used to store backups?

    ☐ Cloud ☐ Secondary data centre ☐ Offline ☐ Within a separate network segment

14. Have the following been implemented to secure the backup environment?

    ☐ Segmentation ☐ Encryption ☐ MFA ☐ Vaulted Credentials

15. Do you use any commercial backup solutions (e.g. Commvault)?

    ☐ Yes ☐ No. Which product(s) do you use: Click or tap here to enter text.

16. Does your backup strategy include the use of immutable technologies? ☐ Yes ☐ No

17. Is the integrity of these backups and your recovery plans regularly tested? ☐ Yes ☐ No

If NO to any of the above, please detail below along with mitigating comments:

Click or tap here to enter text.

Please outline any additional controls your organisation has in place to mitigate the threat of ransomware attacks (e.g. tagging of external emails, DNS, network segmentation, vulnerability scanning, phishing training):

Click or tap here to enter text.

*Signed: Click or tap here to enter text. _____ Name:

*Position: Click or tap here to enter text. _____ Date:

*the signatory should be a director or senior officer of, or a partner of, the Company.