RANSOMWARE SUPPLEMENTAL APPLICATION

E-MAIL SECURITY

1. Do you pre-screen e-mails for potentially malicious attachments and links? ☐Yes ☐ No
2. Do you provide a quarantine service to your users? ☐Yes ☐ No
3. Do you have the capability to automatically detonate and evaluate attachments in a sandbox to determine if malicious prior to delivery to the end-user? ☐Yes ☐ No
4. Do you strictly enforce Sender Policy Framework (SPF) on incoming e-mails? ☐Yes ☐ No
5. How often is phishing training conducted to all staff (e.g., monthly, quarterly, annually)?
6. Can your users access e-mail through a web app on a non-corporate device? ☐Yes ☐ No
   If yes: Do you enforce Multi-Factor Authentication (MFA)? ☐Yes ☐ No
7. Do you use Office 365 in your organization? ☐Yes ☐ No
   If yes: Do you use the Office 365 Advanced Threat Protection add-on? ☐Yes ☐ No
8. Are all employees that are responsible for disbursing or transmitting funds provided anti-fraud training, including detection of social engineering, phishing, business email compromise, and other scams on at least an annual basis? ☐Yes ☐ No

INTERNAL SECURITY

9. Do you use an endpoint protection (EPP) product across your enterprise?
10. Do you use an endpoint detection and response (EDR) product across your enterprise?
11. Do you use MFA to protect privileged user accounts? ☐Yes ☐ No
12. Is a hardened baseline configuration materially rolled out across servers, laptops, desktops, and managed mobile devices?
13. What % of the enterprise is covered by your scheduled vulnerability scans? %
14. In what time frame do you install critical and high severity patches across your enterprise?
15. If you have any end of life or end of support software, is it segregated from the rest of the network?
16. Have you configured host-based and network firewalls to disallow inbound connections by default?
17. Do you use a protective DNS service (e.g., Quad9, OpenDNS or the public sector PDNS)? ☐Yes ☐ No
18. Do you use and endpoint application isolation and containment technology?
19. Do your users have local admin rights on their laptop / desktop? ☐Yes ☐ No
20. Can users run MS Office Macro enabled documents on their system by default?

RANSOMWARE SUPPLEMENTAL APPLICATION

21.   Do you provide your users with a password manager software?   ☐Yes ☐ No
22.   Do you manage privileged accounts using tooling? (e.g., CyberArk)
23.   Do you have a security operation center established, either in-house or outsourced?

BACK-UP AND RECOVERY POLICIES

24.   Is all valuable/sensitive data backed up by the company on a weekly basis?   ☐Yes ☐ No
25.   Are your backups encrypted?
26.   Is at least one iteration of your backups kept separate from your network (off-line)?   ☐Yes ☐ No
27.   Do you use a Cloud based data backup service?   ☐Yes ☐ No
        If yes: Is the service a "hot" back up that is constantly linked to your live environment?   ☐Yes ☐ No
28.   Have you tested the successful restoration and recovery of key server configurations
        and data from backups in the last 6 months?
29.   Are you able to test the integrity of back-ups prior to restoration to be confident it
        is free from malware?

OTHER RANSOMWARE PREVENTATIVE MEASURES

Please describe any additional steps your organization takes to detect and prevent ransomware attacks (e.g., segmentation of your network, additional software tools, external security services, etc.).

Digital signature required below [click the red tab to create a digital ID or import an existing digital ID]:

Sign:
Print Name:
Title:
Company:
Date: