Ransomware supplemental application

Email security

1. Do you pre-screen e-mails for potentially malicious attachments and Links? □ Yes □ No
2. Do you have an e-mail “quarantine service” accessed by all users? □ Yes □ No
3. Do you have the capability to determine if an attachment is malicious prior to the delivery to the end-user? □ Yes □ No
4. Do you have a “Sender Policy Framework” related to incoming e-mails? □ Yes □ No
5. Is Phishing Training conducted for all staff? □ Yes □ No
   If so, how often?
6. Do you use Multi-Factor Authentication (MFA) when accessing e-mail remote? □ Yes □ No
7. If your organization uses Office 365 do you utilize the Threat Protection add on? □ Yes □ No

Internal security

8. Do you use an “End Point Protection” Product across your organization? □ Yes □ No
   Including Detection and Response?
9. Do you use Multi-Factor Authentication (MFA) to protect all users? □ Yes □ No
10. What percentage of your organization is covered by scheduled vulnerability scans? □ Yes □ No
11. In what time frame do you install critical patches across your organization? □ Yes □ No
12. Do your users have local administrative “rights” on their computers? □ Yes □ No
13. Is a Password Management Software (such as “Dashlane”) provided? □ Yes □ No
14. Are your security operations “in-house” or “outsourced”? □ Yes □ No

Back up and recovery policies

15. Are all back up systems encrypted? □ Yes □ No
16. Are your back up files kept offline, or in a Cloud Service? □ Yes □ No
17. Have you tested restoration and recovery of key server configurations and data from backups in the last six (6) months □ Yes □ No
18. Are you able to test the integrity of backups prior to restoration to be Confident it is free from malware? □ Yes □ No

If your organization takes any additional steps to detect and prevent ransomware attacks *(e.g., Segmentation of your network, software tools, external security services, etc.)* please list below:

I understand and acknowledge that the statements and answers are true, accurate and complete and that the information submitted in this supplement becomes a part of the DUAL Cybersecurity Insurance application and is subject to the same representations, fraud warnings and conditions.

Signature	
Title	
Date	