Guidance for Avoiding & Responding to Ransomware Attacks

Business Email Security:

1. What type of email application does your organization use? ☐ On Premise ☐ Hosted/Cloud-Based
   If Hosted/Cloud-Based - What is the name of the product? _____
   If Hosted/Cloud-Based - Have you enabled all default logging for email including audit and mailbox logging? ○ Yes ○ No
   If Hosted/Cloud-Based - Have you implemented one or more of the following email authentication standards: DMARC, DKIM, SPF? ○ Yes ○ No
2. Do you use Office 365 in your organization? ○ Yes ○ No
   If "yes" to the above question – Do you use the "Advanced Threat Protection" add-on and "Multi-Factor Authentication" for all users of Office 365? ○ Yes ○ No
3. Do you filter incoming emails for malicious attachments and/or links? ○ Yes ○ No
4. Do you use email to store, process or transmit sensitive Personally Identifiable or Health Information? ○ Yes ○ No
5. Do you have a formal email retention policy? ○ Yes ○ No
   If "yes" to the above question – what is the maximum duration of email retention? _____
6. Do you allow users to access email inboxes from the web/remotely? ○ Yes ○ No
   If "yes" to the above question – do you require multifactor authentication? ○ Yes ○ No
7. Do you strictly enforce SPF ("Sender Policy Framework") allowing you to publish trusted IP addresses for your domain? ○ Yes ○ No
8. Are external emails tagged to alert your employees that the email originated outside the organization? ○ Yes ○ No
9. Does your cyber security awareness program include phishing training and testing? ○ Yes ○ No
   (If "yes" to the above question, how often are phishing exercises conducted (monthly/quarterly, etc.)? _____
10. Have you disabled support of older email protocols such as POP, IMPA, SMTP and others? ○ Yes ○ No

Internal Security

1. Do you use malware protection or EDR (Endpoint Detection and Response) tools? ○ Yes ○ No
   (*Common EDR tools include Carbon Black Cloud/Cisco AMP/Cylance/Symantec EDR*)
2. Do you use multi-factor authentication to protect privileged user accounts? ○ Yes ○ No
3. Do you have a secure/hardened baseline configuration which is regularly reviewed and updated by someone with security expertise and in line with security industry standards? ○ Yes ○ No
   (If "Yes" to the above question, is this baseline configuration materially rolled out across servers, laptops, desktops and managed mobile devices)? ○ Yes ○ No
4. Do you have established processes for rapidly applying critical security patches across servers, laptops, desktops and managed mobile devices? ○ Yes ○ No

Back-Up and Recovery Policies

1. Do you provide regular (monthly, at least) backups of server configuration and data? ○ Yes ○ No
2. Are your backups encrypted? ○ Yes ○ No
3. Are your backups disconnected from and inaccessible through the organization's network? ○ Yes ○ No
4. Do you test the successful restoration and recovery of key server configurations and data from backups? ○ Yes ○ No
5. Do you use credentials unique to backups that are stored separately from other user credentials? ○ Yes ○ No

Other Ransomware Preventive Measures

Describe, below, any additional steps your organization takes to detect and prevent ransomware attacks:
(e.g. segmentation of your network, additional software tools, external security measures, etc.)