Cyber Security Checklist

1. Do you perform monthly backups of business and financial information and store it in a secure, off-site location, such as a safe deposit box or a reputable cloud-based storage service?  
   - Yes  
   - Needs Attention

2. Do you have policies in place to protect confidential information like contribution records, counseling notes, and other sensitive information?  
   - Yes  
   - Needs Attention

3. Do you have policies in place to report a data breach in accordance with state law and to protect your ministry from legal action?  
   - Yes  
   - Needs Attention

4. Do you have policies in place to maintain compliance with Payment Card Industry (PCI) rules for use, processing, and storage of credit card information?  
   - Yes  
   - Needs Attention

5. Do you appoint a senior staff member who has responsibility to ensure security policies are in place and followed?  
   - Yes  
   - Needs Attention

6. Do you limit access to sensitive data and systems to authorized individuals and is that data password protected and/or encrypted?  
   - Yes  
   - Needs Attention

7. Do you change passwords for user accounts and cloud services on a regular basis and when an employee leaves?  
   - Yes  
   - Needs Attention

8. Do you enforce or encourage the use of two-factor authentication for access to email, church records, and other sensitive data?  
   - Yes  
   - Needs Attention

9. Do you provide or encourage the use of a password manager (like LastPass, 1Password, Dashlane, etc) so those who login to your systems can use unique and complex passwords?  
   - Yes  
   - Needs Attention

10. Do you work with a qualified staff member or computer support company to secure your computer systems?  
    - Yes  
    - Needs Attention

11. Do you update your operating system for security reasons?  
    - Yes  
    - Needs Attention

12. Do you update virus and spyware protection on systems, devices, and applications?  
    - Yes  
    - Needs Attention

(Continued next page)
<table>
<thead>
<tr>
<th></th>
<th>Yes</th>
<th>Needs Attention</th>
</tr>
</thead>
<tbody>
<tr>
<td>13. Have you installed firewalls that are designed to prevent unauthorized access to your computer network?</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>14. If you offer wireless internet access to your attendees, have you created a separate, private network for the church’s administrative computers?</td>
<td>O</td>
<td>O</td>
</tr>
<tr>
<td>15. Do you protect against objectionable or illegal WiFi use by blocking questionable websites, password-protecting the wireless network, and asking users to agree to an Internet Usage Policy?</td>
<td>O</td>
<td>O</td>
</tr>
</tbody>
</table>

Notes: ________________________________________________________________

______________________________________________________________

Completed by: ________________________________ Date: ________________