1. **Staff education**
    - Cyber provider should be sending fake phishing emails to see who clicks on the link in them.
    - Cyber provider should provide 1 to 2 short educational videos per month, monitor who watched them, and send a report to you.
    - Some aspect of cyber should be part of each staff meeting – preferably monthly.

2. **Monitoring of your network and all devices should be ongoing and automated**

3. Proactive protection

- Have a plan in place now, before an incident happens
- If you are using a Managed Service Provider to monitor your network and provide IT services, included in the software they are running on each device should be these 5 things, at a minimum:
    - Use EDR (Endpoint Detection and Response) virus protection – not protection that is based on a library or known viruses
    - Block access to harmful websites
    - Patch updates keeping your critical software up to date
    - Report failed login attempts
    - Detection of PII (Personal Identifiable Information) contained in the content of documents located on local computers. The files containing PII should be reported to you for deletion.

4. **Continuous reporting –** Your Managed Services Provider should provide a report to you monthly (at a minimum; weekly is better) that will inform you of the following items. These should indicate the employee involved, where applicable, and the issue(s) addressed with the employee.

5. **Recover & Restore –** You should have a backup of information stored on your local network, including the "C:" drive of every PC on your network. Any documents should be backed up and a backup "image" of each device used on your network should be included. This will allow you to restore an entire desktop back to its original state quickly with all programs already installed. We recommend your backups be stored both locally and in the cloud.