Module 8 – A basic checklist of technical best practices

The following provide some security controls that should be considered regardless of your technical context.

Network Security

The following are some basic and cost-effective solutions that will help protect your business systems and data.

- ☐ Turn on automatic updates for all software applications and operating systems on all computers and mobile devices.
- ☐ Create strong cybersecurity policies and procedures and ensure that they are communicated to all staff and are enforceable.
- ☐ Turn on multi-factor authentication on websites and cloud services wherever possible.
- ☐ Install anti-malware software on all computers and mobile devices.
- ☐ Backup all of your data
- ☐ Keep an up-to-date inventory of all hardware assets and software installed on them.

Endpoint Security

Endpoints such as computers and mobile devices are typically the entry point to networks for attackers. Below are steps you can take to secure your endpoints.

- ☐ Identity all the endpoints on your network such as servers, desktops, laptops, mobile devices, printers and IoT devices.
- ☐ Ensure anti-virus / anti-malware software is installed on all devices.
- ☐ Enable software firewalls on all devices such as servers, desktops, laptops, and mobile devices.
- ☐ Change the default Administrator password on all devices and applications.
- ☐ Use virtual private network software when using public networks such as coffee shops or hotels.

Data Security

An inventory of your data and where it resides is equally important as completing an asset inventory to know what hardware and software you have installed.

- ☐ Perform an inventory of all corporate data to locate where it resides (i.e.: local computers, local server, or cloud applications)
- ☐ Categorize and classify the inventoried data. Refer to regulatory or contractual obligations to ensure data is being categorized correctly.
- ☐ Assign user permissions to the data based on their job roles, and category and classification of the data. Remember, “Only the right people, have the right access to the right data, for the right reasons.”