WIRELESS ACCESS POINT SECURITY

Data Security

Lecturer: Mark Gillan

CONSIDER SECURITY ENHANCEMENT CHECKS

To help you all think about Hardware and Software changes that can be made to enhance security for Wireless Access Points / Routers

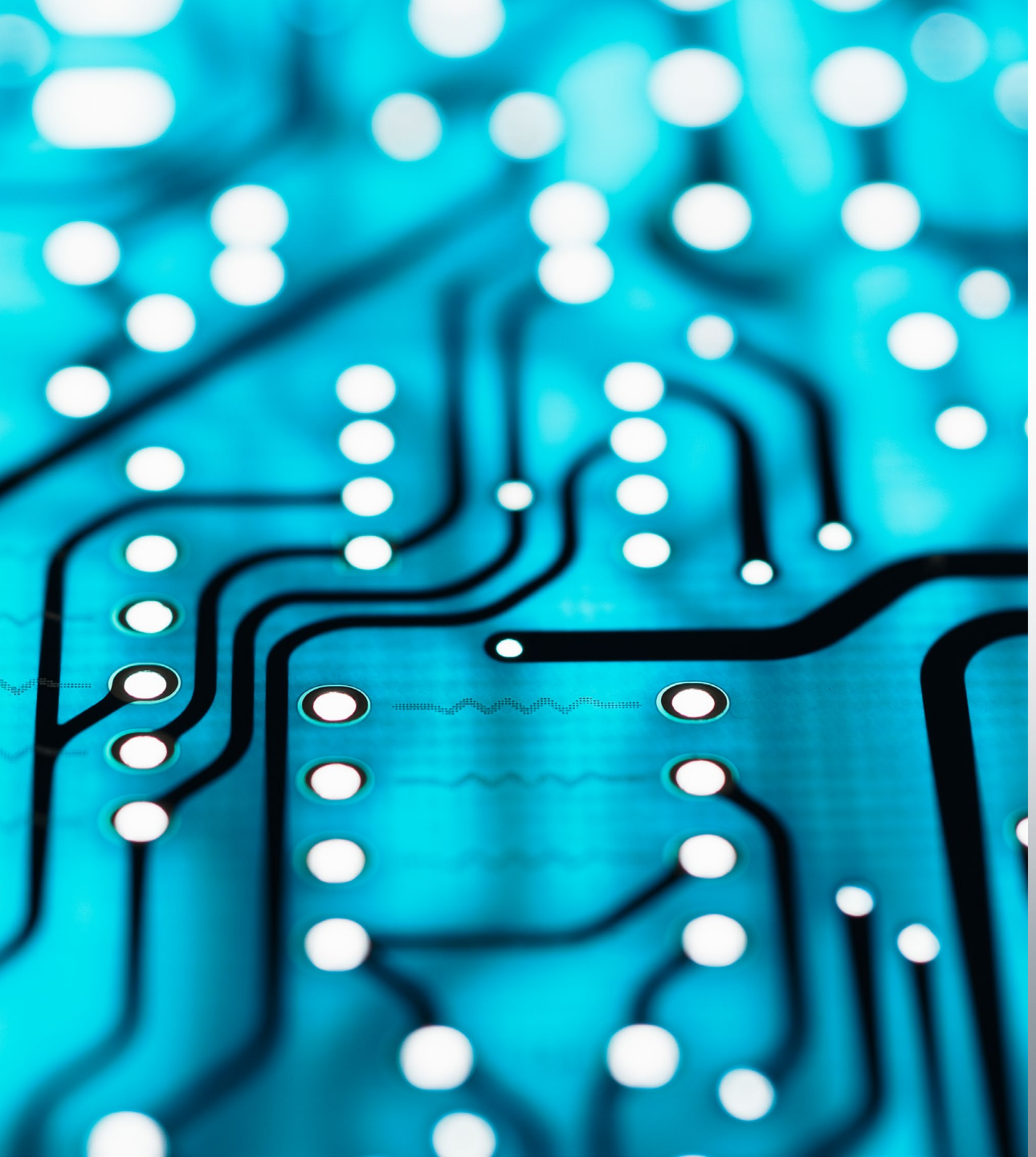
A few points to consider upon the next couple of slides…

HARDWARE

- Hiding the SSID
- Restricting Access to Specific named devices, for example, restricting access to devices that are connected or have recently been connected
- Prohibiting some devices that have attempted or are connected to WAP / router that you don't want connected (an invader, hacker, dangerous device)
- Inbound / Outbound port access restrictions (not allowing guests full access to all ports, for example, not allowing FTP or other connections)
- Changing and upgrading Firewall rules (monitoring, blocking certain traffic, changing what is allowed or not allowed for the Firewall)

SOFTWARE

- Authentication, such as password or PIN requirements for users or tokens for guests, also length of passwords with special characters
- Activate Encryption (WEP, WPA, WPA2)
- Logging and monitoring activity
- Blocking certain sites (black list) or blocking everything except for certain sites (white list)
- Additional software to monitor, alarm /alert. Specialist security software.



IMPORTANT NOTE

Investigate and consider your own security.

Make a note of how your settings are prior to any changes and be sure of the changes you make.

Note, I or the college must not be held responsible for any changes or damage in relation to equipment outside of the college campus.

It would be advisable to note everything as working first and make a note on paper as to changes you might propose to enhance security.

The slides in this presentation are only advisory and any changes to your security must be your own responsibility and you take full responsibility therein.