CO2508 Computer Security  
Risk Assessment & Management

### Scenario

You are the module leader for ‘CO2508 Computer Security’ and are considering how to run the practical exercises that involve using operating systems such as Kali, Caine and Ubuntu. You have access to a specialist ‘cyber security lab’ within the C&T building (CM026), however students can also connect to the network on personal devices via the wireless network.

In the Spring of 2020 the corona virus international pandemic caused the shutdown of University campuses across the world and there was a sudden shift of teaching that went from in-the-classroom to Microsoft Teams, and a reliance on students installing software on their own machines.

Risks:

1. Installing software and configuring it incorrectly due to the lack of knowledge could result in the users opening their network for potential attacks coming from the WAN interface.
2. The users could hack their own devices potentially resulting in a device that is open to the WAN. Eg. Opening ports using UPnP
3. The users could use the software on a device or network they are not authorised to use.
4. Users skip or do not engage with the content/Teams.
5. The user’s internet or power cuts out, making the content unavailable for them.
6. Due to software that could be configured incorrectly, the user could cause irreparable damage to their or other people’s devices.
7. The user’s machine is compromised and an unauthorised third-party gets access to the tools and content the user was working with.
8. Users purposefully attacking their own hardware, resulting in damage.
9. People being malicious.
10. Routers with outdated firmware can be exploited more easily than more advanced equipment that university has.

Impacts:

1. The user’s information and hardware could be hacked by unauthorised parties, resulting in loss of data or hardware damage. Quite unlikely, as users would likely not change their network settings.