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 Routers with outdated firmware can be exploited more easily than more advanced equipment that university has.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.
2. An unauthorised party could change a part of a system that will let other parties to connect to the user’s machine through an open port. This is unlikely as a user would have to install malicious software that would pose as a server for others to connect to.
3. Using a different network to perform illegal activities could be used to blame the owner of the network for the user’s actions. Depending on the party’s Wi-Fi password strength, this is highly unlikely.
4. Due to a home environment, it is very likely some users would choose to intentionally not engage with certain tasks.
5. An internet outage results in users not being able to interact with university content, but the users can make up for it in their own time. Power outages are unlikely.
6. Running a password cracker could cause the user’s device to overheat, if a large password set is chosen. Quite likely, seeing the nature of this module.
7. Even the default antivirus software on Windows can viruses or compromising software. The risk is still likely to happen if the users are instructed to download tools by name only, and not given a link to a direct download.
8. The university will not be responsible for user’s choices. It can be seen as likely if the users want to experiment and learn on their own.
9. Some people will always be malicious. Could result in other users being hacked, but this is unlikely.
10. A typical home router is running out of date Linux distributions. A compromised router can control every piece of the user’s data they wish to send online. Advanced hackers could exploit outdated firmware easily unless distributions like OpenWRT are installed and kept up to date. The threat is quite unlikely, but more and more router hacks are happening.