Hello! Today Huraira and I will be telling you about Physical Security. Firstly, we will help you to understand the Onion Skin model. The onion skin model is a metaphor for the complex structure of information systems. The system is split into layers to make it easier to understand. The first layer is a protective layer like a fence/wall that blocks any incoming threats. The second one is the perimeter layer like a door which filters out who can access the building. In the perimeter layer there is also external and internal building security such as CCTV.

Now, using the onion skin model, we will be analysing the physical security of room 224. First, let's talk about the perimeter fence/firewall. Our school has a firewall that prevents students from going to unauthorised websites. This also helps with securing our network from any remote threats. In terms of external building security, all the rooms in our school are able to be locked to keep intruders away. The school is also equipped with external and internal CCTV Cameras. For our room in particular, there is a sign in sheet (internal access control system), and there is also teacher supervision (passes and guarding). This proves that our classroom passes in the eyes of the onion model, making it a positive example of physical security.

While we were reviewing our room through the onion model, some questions arose. These include:

1. Are there CCTV cameras inside the lab?
2. Who will have access to the lab?
3. How is the room secured when it is not in use?
4. Who supervises the lab?

We have many choices for people we can turn to to answer these questions. Pick a Mr. Henrich and ask away! If one of the Henrich's are not available please ask an IRHS IT personnel.

There are many aspects of a network that Physical Security addresses. For example, there are many ways that a hacker can do damage to a device if they have physical access. There is a small device called USBkill that can render a device useless if it is plugged into it. This poses a serious risk for any computers that store data. You wouldn't want your project files getting deleted because the building wasn't secured, would you? For our room in particular, a USB kill could result in many people's personal devices getting destroyed. Although devastating, the USB kill is not the only threat that is caused by bad physical security. A rubber ducky is a device that is used for logging an infected user's keystrokes. There are a few things in common between the ducky and the USB Kill. Both of them are serious threats because they are undetectable by antivirus software and the user is unlikely to notice it. In both cases, the damage could be avoided using physical security, whether it be CCTV, guarding, access control systems, or anything else.

When building a computer lab, should physical security be considered? The answer is undoubtedly, YES! However, that explanation does not contain much detail so let's try again. *Why* should physical security be considered? For starters, all doors and windows should be sturdy and secured. It is also essential to have a good surveillance system, not only to record what happens in and outside of the room, but also to deter blatant crimes inside the room. There must also be a system for checking who is inside the lab, such as a sign in/out sheet or some sort of keycard system.

Thanks for listening to our presentation. Have a great day!’
Thank you!