**The Human Factor**  April 2022

Outline of presentation

Present your solutions to the issues identified in Unit 3

Including – Social and Ethical considerations

10min presentation  
With transcript of the audio file

**Learning Outcomes**

Critically examine effective strategies to promote and manage the human factor in cyber security.

Critically evaluate the social and ethical considerations in developing and applying usable security.

-----------

Hi Oliver,

As you kindly suggested I will focus on the potential solutions for the issues that I raised in the essay:

**Training and awareness**

* Focus on fun impactful cybersecurity training.
* Looking deeper into the way people think to help aid in understanding the best course of action regarding training.
* Not all cybersecurity training will work for all staff members in all departments.
* Using a developed adult learning principles to maximise content retention.

**Cyber culture**

* A good focus will be that recognising that people make an organisation secure, not the technology you have in place.
* Fostering an environment where the employees have the knowledge and instinct to be the first line of defence.
* If an official policy makes it hard for someone to do their job, people will find a work around to carry out a particular task.
* Without a healthy security culture, staff won’t engage with cyber security, so you won’t know about workarounds or unofficial approaches, creating an inaccurate picture of the organisation’s cyber security. Thus, missing the opportunity for valuable staff input about how the policies and procedures can be improved.
* Develop a ‘just culture’ where staff are encouraged to speak up and report concerns, appropriate action is taken, and nobody seeks to assign blame.

**Stake holder and leadership engagement**

* Board members set the tone in cyber security by leading by example within the organisation.
* There should be no special treatment around senior members of staff, if the policies don’t work for senior members, then this should be worked through with the policy makers.
* Properly resource staff awareness.
* Staff input in included when creating new policies or system designs.
* Ensuring staff feel empowered and have an easy way to raise security concerns at any level in the organisation.
* Take responsibility for you own role, by recognising the risk you pose as a likely target (Whale) for attackers and should take the appropriate measures to act accordingly.
* Speak openly and positively to staff about why cybersecurity is important to the organisation.

I will also record a video of the slides with audio on top of it using power point and present.

I shall not address the zero-access policy, as you stated in your comments of my essay that is an approach which may not be beneficial.  
  
Do you think cyber culture and stake holder leadership fall under the same section?

Thank you for taking the time to review this document.