**Unique Identifier: ST3**

**General comments:**

Did not take on any actions really but was definitely more mindful of stuff after it. Even told his friends about using a sentence as a password.

**Action 1: Backup critical data regularly**

He works with audio files a lot. Uses mac book for first time for the iCloud back up service… hates it. Was also using iCloud for the primary copy of his data which was a big mistake.

**1)** It’s okay, nothing very new to me. The step about critical data sets is crucial, identifying what that is different / difficult in my case.

**2)** Yeah I would say so

**3)** I’ve never been in charge of a company’s data back-ups before, I’m staggered with difficulties with it myself over years. I find it overwhelming. Does a backup on USB for photos on personal phone.

**4)** Has so many files it is hard to back up so many large files.

**5)** A lot of text there it’s just a busy slide, that’s what’s coming to mind. Maybe some images or icons.

**Action 2: Always use MFA**

Most of the first part is fine, I’m kind of losing it a little bit at number 4. I don’t know how to apply encryption in everyday life.

**1)** Largely I’d be in favour of that. Fluctuating between my work and personal life, there are some things that require mfa and it can be annoying. I’ve been using a VPN and it asks me to input the password of the computer each time which was too much I thought.

**2)** Everything else is clear and easy except point 4.

**3)** I think so yeah

**4)** Yeah, the licensing thing I had to use didn’t have the option on the free version.

**5)** Just point number 4 separate it into different points/sub text instead of one big paragraph. Encryption is a techy term so more explanation or maybe a link.

**Action 3: Maintain a cyber incident response plan**

Wouldn’t have thought about this before the workshop but have definitely thought about it since.

Would be great if there was a template to follow

**1)** Definitely needed

**2)** Very high level

**3)** No because it is too high level at the moment

**4)** Not enough information given

**5)** A template to be given, more explicit advice.

**Are they tailored to your business?**

**Are there any other cyber risks that you are surprised weren’t in your top 3?**

Nothing is jumping out at me no

**Any feedback/questions:**

Happy to be contacted again.