**Feedback on risk assessment tool**

detailed

sometimes you could answer a questions there – when you are getting rid of a deivce, do you wipe it – maybe we think we wipe it, but we might not have.

feelings of cybersecurity changed

They are good questions.

* some comment at end “everytime you tick something it throws up another one.”

Data backups

* drives – connect one to server throughout the day – the software has automatic backups – take one out in the evening in case of a fire
* But we are always worried about ransomware , apparently they wait a few weeks so they have all your backups.

Question on backups – “I am making copies of the files, is that the same thing?”

Other cloud providers = iCloud

**Question after backup presentation:**

Would you have a checklist to avoid what happened that florist.

Here is how to avoid the common pitfalls. For SMEs know what the main things they should do.

Question about 2FA if you don’t want staff to have to use their own phones – yubikey (We should include this in the list)

What should you do if you have done something wrong – if something has happened. Do you have steps we should follow

* want a general information checklist.
  + on wh

Someone accessing remotely – our recommendation is VPN

Someone asked what about Team Viewer?

Question – how to improve employee culture

Look at what the norms are – without blame.

# Splitting wifi – guest versus actual

pinging systems – really powerful, I never though about it like that.