# Kerry Workshop 30th April 2024

## Participant Backup on Data Backups

* Good awareness of ransomware.
* Questions on IP (Intellectual Property) – what is it?
* Data Backup Frequency – link the backup frequency to cost…if we had all the money in the world, we would have full time backups but that’s not realistic, we need to balance money with backup frequency.
* Backup Frequency slide – it would be good to differentiate between different types of business – say, a pharmacy couldn’t afford to lose days worth of data because it would be dangerous for clients, and not compliant. But maybe a hairdresser or florist could do without data for a few weeks.
* Question on ‘what are backups’ – are they just copies of the files? Review backups on tables/data etc. Some backups are not just copies, they backup the changes in tables.
* NAS box – it’s useful as a ‘2nd form’…you need 3/2/1. So you could do NAS box plus cloud. It does have a use for bigger companies.
* Participants did not know that ransomware can encrypt your Cloud Data – lots of interest in the comment that if you have ransomware on your local machine, it could infect your Cloud through a sync.
* Cloud Storage v Cloud Backups – it would be good to say that we all rely on Microsoft and Google never to be hacked, and that’s a pretty reasonable assumption but if your local machine is hacked, your cloud data can be impacted.
* I really liked the comment on ‘what we are giving you today is the right language’…to talk to an IT expert – immutable backup and air-gapped. That resonated with Participants.

## Participants Feedback on Access Management

* We could comment on the fact that password advice has changed so much – we used to hear about having special characters etc. but now you can go with a long sentence. Should we say 16 characters +.
* When we ask about the ‘sophisticated phishing attack’…if no one has experienced it, give them an example – CEO Fraud. Use the Apple Gift Card example.
* Prevent Phishing Attacks…bring it home by mentioning friends and family – they could get caught if they are working in the business. Don’t assume all staff, family and part time employees are as cautious as you.
* On the MFA – we should explain that it is prompted by the Software Application or the platform you are using. You can’t ‘put’ MFA on yourself.
* UB Keys. Hardware tokens. Option to use instead of Authenticator – which is generally on a personal phone.

## Admin

* Some people had Issues with the broadband/WiFi and filling out the Risk Assessment Tool.
* Issues with tech – projector. Fixed by hotel quickly.
* We need a count down clock for the ‘Before Survey’ and the ‘Risk Assessment Tool’.
* It really helped the Participants during the Data Backups when Brian talked them through the questions as they were answering them. We need to avoid silence as much as possible.
* The slide ‘Data Recovery After Cyber Attack’…we need to make the words bigger (in the arrow)…you can’t see the words from the big screen.
* Send a copy of the slides to Fiona so she can distribute to the Participants.
* I’ll send Top 10 Tips for SMEs to Fiona.