**Unique Identifier: B6**

**General comments:**

Workshop gave him something to think about, payroll information started using encryption for those documents.

Double check things, and is more mindful after the workshop

Gave him a renewed enthusiasm

Not to presume that the people he works with hasn’t been attacked

necessary to take advice seriously and don't assume everything is correct

**Action 1: Backing up data**

1)Perfectly reasonable, perfectly doable. Formalising the backup procedures, perhaps having an External Hard drive.

2) I would be able to follow the steps

3) Did seem clear and helpful, nothing I didn’t understand

4) shouldn't be any barriers, there's a will to do it. Might have to buy an external hard drive. Could do cloud backup. In between things at the moment, changing the website.

5) Makes sense to me, language is understandable to most people working with a computer in this day and age

**Action 2: Cybersecurity training**

‘Seems reasonable’ ‘what would it cost for training?’ (thinking in line of a fire safety person who came to give them training, could someone do this but for cybersecurity?) Mention incidents from the news or just examples of cyber incidents, doesn’t have to be local, would be interesting to have like 3 examples of things that could happen, only really hear of big ones like the HSE. Raising awareness.

1) Appropriate, same way we do fire safety, we should also be looking at cybersecurity, should be part of training and safety, wasn’t anything complicated there.

2) Yeah

3)

4) I don’t know what you would be looking at in terms of cost 600-700 euro. What would it cost? touch wood we’ve been lucky but that can change any moment. Sometimes you're less careful than other times and it can happen

5) Maybe put links to some free resources, maybe information as to whether it would be better to go with a third party training company.. probably better than myself trying to give training

Mention incidents in news, not many incidents reported unless its bigger businesses such as hse. It would be interesting to have 3 examples of the kind of thing that can happen. Alert – This incident happened this week. Cybersecurity awareness - not popular.” Nobody’s going to come for us “

**Action 3: Ensure website is backed up**

We are changing things up; I will bring in good housekeeping practices. We will be backed up to a certain extent, but it was something we were discussing. If something happened to your website, you could switch to a new version of it. - Cost

Potentially switching websites, will be changing things up so it’s time to bring in good housekeeping and good practices, website back up is something they were discussing with the company.

1) Yeah perfectly reasonable

2) Seems clear and helpful

3) Yeah, it is a matter of looking at a few things and contacting the host so there’s nothing too complicated with that

4) Shouldn't be any, someone should be able to, hopefully the host will help.

5) Don’t think there’s anything I can suggest to improve it necessarily

**Are they tailored to your business?**

Yes I would agree that they all should be priorities, I want to run with this. I’m glad to have these few things, will certainly push them.

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

Can’t think of any, those are a lot of the main areas. The training provides a focus on things to look out for and good practice and stuff like that. I wouldn’t say there was any surprise there

**Any feedback/questions:**

I would agree that all of these should be priorities, and I will run with it. We will implement these things and have good housekeeping.

Those are the main areas really, the training provides a focus on things to look out for, good practice. It wasn't a surprise.