**Risk Assessment Tool Pilot - Ross-20240404\_150333-Meeting Recording**

0:02  
OK.

0:02  
So feel feel free to work away whatever you need and then we'll we'll go through together.

0:05  
So Mary, So what we're hoping for for this activity is just basically a think out loud activity.

0:11  
So the questions that you come across, just what your thoughts are on them, are they relevant, how that could we improve them or whatever comes to mind is basically what we're looking for with this perfect, perfect.

0:23  
So I'll just read the first bit here.

0:25  
And yeah, that's fine.

0:31  
Yeah, that's fine.

0:34  
Perfect.

0:34  
That's grand.

0:34  
So, yeah, Sachin is in perfect nature.

0:40  
That's grand.

0:42  
Yeah.

0:44  
Yeah.

0:45  
That's no problem.

0:48  
Yes.

0:49  
OK, let's go.

0:52  
So are you so trader?

0:53  
No, how many employees are in the business all time including all part time and full time staff.

1:01  
I would put it at we're going to do 185 for the moment.

1:06  
It fluctuates as you can imagine construction depends on on the projects and and whatnot as well.

1:11  
So construction that's fine.

1:14  
Who manages Social Security for your business?

1:19  
So now probably here is probably one that I would say is a bit ambiguous because like who manages cyber security?

1:25  
Like obviously I would probably put in myself, but do you know, does that capture exactly what the people are doing in terms of do you know where I'm coming from?

1:32  
Like, umm, you know, you could say myself in an IT capacity or I'm part of an IT team or do you know something like that?

1:41  
Umm, because I have seen companies where cyber security might be dealt with, like maybe the legal department, you know, there's somebody who might be like technically minded in a legal background who deals with it.

1:49  
Umm.

1:50  
And that was saying people would do with GDPR and things like that as well.

1:53  
Umm.

1:53  
So maybe just in in terms of that, Umm, cause like, you know, that's kind of maybe overlapping with .1.

1:59  
Dedicated service security person team in house.

2:02  
Umm, technically you could argue I'm a dedicated person, but I'm also dedicated to a lot of different things in the IT department as well.

2:09  
So you know, it, it just kind of just depends on umm on what's needed.

2:13  
Umm.

2:14  
And then maybe for the second one as well, an outsourced person or team, like maybe you want to maybe clarify, is it a cybersecurity outsourced person?

2:22  
Is it an outsourced person?

2:24  
Who do you know what's what's their speciality?

2:26  
Is it just somebody who who deals with cybersecurity?

2:28  
It might just be better just in terms of data logging, Do you know who, who specifically it is?

2:35  
So I'll just do myself anyway for the moment.

2:37  
And sure, you know, I'm an IT manager anyway.

2:39  
Umm, so cyber insurance?

2:40  
Yes, we do.

2:41  
This was a this was a huge thing umm last year, umm, because it's obviously become far more relevant.

2:47  
And that's E exactly why when I was chatting to Miriam last year and we were probably either in the thick of it or just after it.

2:53  
So we've only just recently renewed it as of a few weeks ago and they're actually asking a lot more information.

2:59  
So we go through a brokerage firm and it works quite well because we obviously get you know different different styles and and things of what's needed.

3:06  
But like at the moment now I think the big thing that they're looking for this year is what is your data retention destruction policy.

3:14  
So we we had one, but we didn't have anyone kind of set out in stone as such.

3:18  
So I had to do that over the past number of weeks.

3:20  
Do you know along with the directors.

3:21  
So that's just maybe just something just to keep in the back of mind is, is, is kind of what's happening.

3:25  
So does your business currently meet the minimums out here?

3:27  
Yes, it does.

3:29  
Can customers make purchase on your website?

3:34  
I have a website, but yeah, nobody can make purchases.

3:36  
How is your business website managed or maintained?

3:42  
That is a really good question.

3:44  
OK, so I'll I'll tell you what we do Miriam and you can a you can probably answer which one I should choose.

3:50  
So we have a company called Orpen Design Solutions and they are a design consultancy, but I and the IT department deal with the upkeep and maintenance of the website itself.

4:03  
So when you say how is your website being managed or maintained, they're probably 2 separate questions, I would say.

4:10  
So like, you know, like do you know what I mean?

4:12  
Like maintaining a website would be us.

4:14  
We upload the news items, the data and things like that.

4:17  
Who's managing it?

4:18  
You know, maybe us from a cybersecurity standpoint, but like we outsource to them.

4:23  
Then any of the design consultancy, if there's any changes in terms of SSL certificates, do you know that kind of stuff we we would do it to them.

4:30  
So I mean, umm, it's up to yourself what one you think I should choose for that or you know maybe if if you're doing the questions, I would probably either split it up into two different questions, who's managing and who's maintaining or else maybe just tidy up the question a bit and and maybe just change the word manage and maintain to to something else.

4:47  
Do you get where I'm coming from?

4:48  
Yeah, no, I'm making note of that because I will change that because that is valuable.

4:53  
I'd say for now maybe if, umm, if we say I manage and maintain the website, yeah, that's grand.

4:57  
But I'll, I'll actually split that question into two.

5:00  
Yeah.

5:01  
But you get where I'm coming from just because just in terms of business, it does IGV conference, umm, yeah, we do.

5:06  
So now maybe something might be here as well because I see you have breakout questions depending on what you answer.

5:12  
Umm, a nice one here and we actually had to do it as part of our initial cybersecurity.

5:16  
Miriam is do you have a backup of your website.

5:19  
A lot of people that actually is a a huge important thing.

5:22  
So people backup their emails, they backup their Dropbox, their, you know, whatever it is.

5:27  
But a lot of people don't make a copy of their website and uh, like we're seeing quite a lot now at the moment, especially in ours.

5:33  
Umm, like if I showed you the, the, the data, you'd be, I think every day probably 30 to 35 people try to hack into our website, umm, every, every single day, umm from all around the world, Umm.

5:44  
And that's just, I mean we're now we're, we're getting bigger as a company, but like that's just to put into perspective.

5:49  
And so we, we back it up every 12 hours.

5:51  
So we do it in the morning and then after work then as well just in case there's any changes.

5:55  
But that might be a question because, um, from my experience, I would have never thought of something like that unless it was in the brokerage thing to say, Do you, um, back it up now we pay six year or a month to back it up.

6:06  
It's like the cheapest thing in the world, but it's actually the, the aspect of doing it and umm, you know, checking your disaster recovery and things like that.

6:12  
So it might be worthwhile maybe just having a breakout question there saying, you know, do you feel confident managing the service security?

6:16  
Yes.

6:17  
Umm, do you have a, a backup of your website or do you currently take backups of your website?

6:21  
Just something simple.

6:22  
And I'd actually really love to see the data on you know, especially breaking out between maybe you know SM ES lower than 2025 employees and then maybe us getting into more the M side of the SME.

6:32  
Umm, are people actually doing backups.

6:34  
So only just a, a small thought on that then as well, umm, do you have an inventory of all of your digital hardware?

6:39  
Umm, yes that is probably and that was a a big thing that we had to do even just this year.

6:45  
As you can imagine construction sites aren't the the best for managing and maintaining their things.

6:50  
So like across the hall is our purchasing department.

6:53  
So they would do a really you know comprehensive inventory, they would do all their off hired and things like that.

6:58  
So we've we've started doing that myself and Kahl who's next to me, we've done a whole kind of survey on what we have, we've done a whole checklist.

7:05  
So they're all asset registered.

7:07  
So you've probably never one second.

7:09  
I'll just show you for a second, just so you can see if I can get this open.

7:14  
One second.

7:17  
So.

7:17  
Oh, and there's not even an asset tag on this one.

7:19  
OK Well, that's not great.

7:20  
We'll start one second.

7:21  
I'll see.

7:22  
Can I find, uh, just just to show you for for argument's sake, because I think it will be handy for so I don't know if you can see that.

7:28  
So every single item in Seafield has an asset tag, it has a number, it has a thing just to doing it as well.

7:35  
So like in terms of thing, I don't know if it's a case that you maybe want to spit that out into.

7:40  
Do you tag your assets like, I mean, I suppose again, I don't know if it's a question that needs to be broken out into.

7:49  
Do you have an inventory somewhere?

7:51  
Yes.

7:52  
Do you currently acetag your items?

7:54  
Like I I don't know if you know, you can put that into a separate questioner or keep it in because I have seen people keeping an inventory.

8:02  
But you know, often times, especially in construction, you're on a site and then it finishes 6 more later.

8:07  
Where does that get allocated to?

8:08  
Does it get allocated to head office or whatnot?

8:11  
So wing system, you have your own monitor, you have your own laptop and then you bring that with you to site.

8:15  
So I just said I'd say that just maybe it might be, might be worthwhile.

8:20  
Yes, that's a big thing.

8:22  
Yeah, maintaining a thing of of, of software in in terms of that question as well, you're probably familiar with SAS.

8:30  
So software as a service kind of things.

8:34  
It would be interesting to see maybe in that question like do people manage and maintain their software licenses And what I mean by that, so I actually have a call and this is actually quite must be burnt on this.

8:51  
And so I actually have a call in about 45 minutes with a company called Zluri.

8:54  
And basically what they do is their product is a digital dashboard that takes in all of your licenses across all the things and basically shows it to the IT manager in an easy readable format.

9:05  
So you can see where things are going.

9:07  
Maybe there might be a question either in this or maybe separately to see, you know, how do you manage your software licenses?

9:13  
Is it through the admin panel of the specific one, Do you have a third party that does it and whatnot?

9:18  
How is the allocation process of those licenses because that would be a big cybersecurity element as well as you know are people just Willy nilly just taking licenses as needed?

9:29  
Like I'm seeing a lot at the moment, some businesses if they're going to the SAS based model, they have what's called pool or collective licenses.

9:36  
I think all CAD calls them flexi licenses.

9:39  
But essentially there might be 10 people in the company that might need to use the software.

9:43  
We pay for two or three licenses and it just allocates them as people in and log.

9:48  
You kind of have an ebb and flow of it.

9:50  
Again, I don't know if it's something that you're looking at in the in the cybersecurity or kind of resilience inside of a Miriam, but it might be worth just to know if we just have a discussion just to see because I know that that's becoming a big item now at the moment just in terms of security, you know who actually has the licenses, who's assigned to, are they using the software effectively all that kind of stuff kind of comes into it.

10:10  
So again, it just might be worth them, might be worth doing.

10:13  
Do you remember the staff use their own personal devices for business?

10:16  
Yeah, Yes.

10:17  
So this would definitely, I would say need a breakout question, Miriam, it's called MDM, so mobile Device Management.

10:25  
So what I would say there is if somebody says yes, do you have Mobile Device management enabled on those personal devices.

10:33  
So basically what that means is they could have Microsoft Intune, they could have, they could have Android Enterprise, they could have a lot of different things.

10:41  
What that means is that although it's a personal device, certain aspects of that device are locked down business wise.

10:49  
So the question yes we do, we only supply Samsung phones, so some people are so against Android that they will use their own iPhone, which I don't mind.

10:56  
But as part of that then as well they can only access certain things with their e-mail, you know, the their e-mail address, the App Store, things like that as well.

11:04  
So it's Commonwealth device management, MDM, it's a pretty big thing.

11:07  
But again from a cyber security standpoint, does the company have an MDM profile, Is it uploaded to personal devices?

11:14  
Do they not, Do they even know what MDM is?

11:17  
I think that would probably be a pretty good question to ask.

11:18  
If they if they say yes, do you have antivirus on your devices?

11:21  
Yes, on all devices.

11:23  
That's fine.

11:24  
Again, this might be another one I would maybe say Now again I say I don't want to be making it too long for you, but I think so.

11:31  
There's a difference between antivirus and endpoint management.

11:36  
So endpoint management is basically similar to device management, but basically it it just scans proactively.

11:44  
So while antivirus is kind of as you're downloading and whatnot, endpoint management is basically, I have it's called Intune.

11:50  
So Intune can be mobile as well.

11:52  
We have certain filters and whatnot.

11:55  
So if people are accessing content or whatnot as well, it kind of covers all that.

11:58  
So it it's not just an antivirus, it's more of like a holistic kind of thing.

12:07  
So again I don't know if if your research is going to go through that, but I mean if you're asked question do you have security tolerance, endpoint management specifically and whatnot.

12:15  
And what I might do is I might not share at the end of the call, I'll, I'll stop sharing my screen for a little while Miriam and I'll see can I fish out, maybe not or completed one.

12:26  
But I might just show you an example of what the brokerage firm was looking for in terms of questions for the thing because I think that would be very handy as well.

12:36  
Just to see what they're actually looking for for in in terms of because it's like it's like 31 past 32 pages it's it's a huge amount of info what they're looking for spam has enabled of course.

12:47  
So maybe you want to just spread that out into spam slash phishing because they're two separate things that you have in your device management.

12:53  
So you have phishing filters and then you have spam filters as well.

12:57  
And yeah, that kind of goes into quarantine in the.

13:04  
So yes, it's managed.

13:06  
I'll manually configure this.

13:07  
So as part of the Microsoft endpoint managing a thing called TP separate to do is we as it says in the question, we manually configure that then specifically to what's needed at sea field.

13:18  
So we have Geo restrictions in place.

13:21  
So if people are emailing from outside of certain countries or whatnot, it'll automatically be flagged as spam or or blocked or whatnot as well.

13:27  
So it's a little bit more granular than just having a filter on it that we can actually change as we go along.

13:34  
Our work twice is yes, exactly.

13:36  
So that's a big thing.

13:39  
So our current workflow and literally Carl is working on one at the moment.

13:42  
Next to us as as we're on question 17 here is that when somebody finishes up with the company, not only are their devices wiped any information that they haven't uploaded to the cloud, so we call it the 3DS documents, desktop and downloads.

13:54  
We take a snapshot of the and we upload it to a portal so that if the line manager needs any specific information, they can access it cloud as well.

14:06  
So again, I don't know if that's the case that needs to be added into the question or whatnot.

14:09  
I've always seen that it's best practice from a cybersecurity point to do that as well in case there's no information lost.

14:14  
And literally a great example is about 20 minutes before our call and somebody finished up with us last week and their line manager rang saying can we have some of the data.

14:20  
So thankfully we we have a backup of it in the cloud.

14:22  
So just things like that as well.

14:24  
Umm, how do you keep the software on the device up to date?

14:27  
Umm we have automatic updates.

14:30  
Umm OK, so TH this would be a good question again.

14:33  
Umm, it's called Group Policy is is the name of it.

14:36  
And basically I'd put in an option there called is Group policy enabled A and what that basically is, is it's a form of MDM for umm, mobile device Management.

14:45  
Umm.

14:46  
And like mobile device by the way, it can be laptop, it can be phone, it can be I.

14:49  
It's not just a, you know, a tablet or whatnot.

14:52  
And what you can do is you can set a group policy that certain updates are installed by default and then others umm, need permissions or or whatnot as well.

15:00  
So an example being is that, umm, like Windows 10 most of our laptops are on at the moment, they do quarterly updates called feature updates, which are fine, that's grand.

15:08  
But then there's important cybersecurity updates and whatnot as well that are automatically added by default and whatnot as well.

15:15  
So it's called Group Policy.

15:16  
Again, just have a a quick look online, you'll be able to see and and maybe just maybe add in a question saying you know Group Policy is enabled for device management or whatnot.

15:25  
But what I will do anyway is automatic updates are on all applications by default anyway.

15:30  
The the only reason maybe I'd be apprehensive with that second option Miriam, is there's some apps that you would never have automatic updates for and the reason being is you don't want them to break because Windows has updated itself.

15:42  
If that makes sense.

15:44  
So there would there would always be conditions where you'd have automatic updates on 8590% and then you'd have Group policy on maybe 10 or 15% of the ones that you're just worried that you don't want them to break for whatever reason.

15:55  
And then in in that instance, Miriam, what you do then is you'd like I have an account manager with a lot of the the big vendors, they'll tell me then, oh, hang on a second, Ross, don't update that.

16:03  
Windows has actually done something.

16:05  
Give it a week, we'll do an update and then we'll roll it all out to people.

16:08  
So you just don't want to be breaking their workflow when they're in the middle of of trying to do work and whatnot.

16:14  
What type of data does your business collect?

16:18  
That is a good question.

16:19  
See, I don't really deal with a lot of the of the data items like we definitely don't do, I'd say personal data definitely because CVS will come in and whatnot as well.

16:29  
Careers, all that kind of stuff, Intellectual property, definitely.

16:34  
A great example is we have a pharmaceutical site in blarney for for Merck Pharmaceuticals.

16:38  
I'm actually going there in about an hour and a half, and when I was flying my drone, umm, I couldn't show certain pipes in the facility because they were manufactured with a certain way that I in case I sent them to their competitors or whatnot.

16:51  
Like certain things like that are are really specific.

16:54  
So yeah, in textual property would be a very big thing for us as well.

16:57  
Umm.

16:57  
So I'd say those two just for for whatnot.

17:00  
Umm, yes, that's fine.

17:02  
Exactly GDPR.

17:03  
So we we had something very similar happen.

17:06  
Uh, Miriam, we we had a breach, but it was an extremely small breach basically.

17:11  
And we have MFA, uh across the whole organization.

17:14  
Everybody has to sign in, umm, with either a code on their phone or else an authenticator app.

17:19  
And there's a new, uh, umm, it's called a man in middle attack at the moment, where if you put in your details for however long the token is on, I think by default it's a day, 24 hours they can get access to your system.

17:31  
So we had one, uh, person that did it.

17:33  
We found out about it within like 47 minutes, 48 minutes.

17:36  
But as part of our thing, we had to notify all of the the clients.

17:40  
Just look, bear in mind this has happened and and whatnot as well.

17:42  
So I think a lot of people don't realize that you're supposed to do that because umm, every, I'd say at least once a week I have to ring an Irish company and say do you know that John has been hacked?

17:51  
And they're like, Oh yeah, yeah, we just didn't want to say it to anybody or whatnot as well it it happens very, very often, which isn't the the best thing in the world.

17:59  
And then I suppose the issue as well, Miriam, as you know is that if someone doesn't tell you, you presume that they're fine because you're you're doing work with them and then that's how it, it passes on almost like you know COVID in a way, umm, if I, if I can say it like that.

18:12  
So umm and and that's how it happened with us is that we were actually dealing with a contractor umm a very specific one on site that was doing a an assessment for us and the UH person in question just clicked on the PDF thinking that it was the assessment and and that's how it happened.

18:26  
Umm.

18:26  
So the the big thing now is umm and I don't know if there's going to be a question on this, I I haven't, you know, we're not at the end yet.

18:33  
Umm, there's a, it's not a new thing, but it's only been out about a year called risk profiles in Microsoft.

18:38  
So we've enabled those for the past six months and it's been so important.

18:44  
Basically what it does is in the background, since we use Active Directory, it creates a profile of Miriam.

18:49  
It sees when you normally log in, where the location is, what apps you normally use.

18:53  
It not like super sensitive data, but enough to kind of make a profile.

18:57  
And then if something out of the ordinary happens, you log in from Zimbabwe or whatever, your score will increase hugely.

19:03  
And we set a threshold, umm, and if it goes over that threshold, you're immediately blocked from signing in or from sending any emails until the IT department deals with it.

19:11  
And then every week myself and Kahal will get an e-mail risk profile breakdown and if there's anybody that needs to be actioned or or things like that and so on.

19:19  
So it's it's only really been in the business, I'd say not even six months, maybe four or five months, UH, specifically after that breach, we wanted to kind of implement it, but maybe that might be something as a question or you know, a follow up or whatnot.

19:30  
It's become really important, umm, as of late, the probably the big question that I was asked, asking the Microsoft representatives is what increases your score and whatnot.

19:38  
And they will refuse to tell you because obviously if they do you're if you're a malicious person, you're just going to do the opposite of of what increases your score or whatnot as well.

19:46  
So it it is, there's there's a lot of false positives at the moment as they're trying to tweak the system, but it's been working really well for us.

19:53  
Umm, it has actually caught one or two things already, which is brilliant.

19:56  
So I only just said, I'd say it to you while it was on the top of my head that, umm, it might be worth something just to to do, umm, so where do you store your data?

20:02  
So cloud storage, yes.

20:05  
Now is, is this in relation to question 20, Is it Miriam Question 21, where do you store this data, The question 2019, So OK, OK.

20:17  
So again I might just maybe say in reference to question 19 or or something like that because I would have thought that it would have been maybe GDPR data that would have been based on it.

20:27  
But I'd say yeah cloud storage is probably the the one thing like you'll see it on again like I know what you mean Miriam here on a work computer but maybe you'd be a bit more specific like on a on the desktop of your computer or whatnot because I mean you could argue that all the data is on a work computer.

20:47  
Do you know what I mean?

20:48  
But I know where you're coming from and the answer is like is it on a non cloud thing or is it just sitting on your your thing like we're very specific at sea field like you can't be having any work stuff on your desktop and if not then it has to be in the cloud.

21:00  
But a again maybe just maybe just tidy up maybe the thing I I know exactly what you're on about though in terms of do you encrypt the data you store.

21:06  
Yes all data is encrypted.

21:08  
So a again this is a bit of a loaded question because all data just from any service will be encrypted by default by it's probably S HA256 or something like that.

21:21  
Maybe what you're trying to ask there is like, are we specifically encrypting it or are we looking for a service that will encrypt the data?

21:28  
So like by default, Umm, like the two main places that we stored is in, uh, Dropbox and uh, a company called Procore which specializes in construction document management.

21:38  
Umm, the reason we went with them is they encrypt everything.

21:40  
They salt and hash all the stuff and whatnot as well.

21:43  
But like if I go to a random company, the expectation is that they'll encrypt it anyway.

21:48  
You know, I'm not going to be asking do they encrypt it.

21:50  
So again, it's maybe what are you looking to actually get from that question?

21:54  
Because I would say 99% of people are going to say yes, all data is encrypted because it should be by default.

22:00  
Umm, maybe the the questioning there is like do you understand the need for encryption or do you know are you aware of encryption for that in general or whatnot?

22:10  
Like a great example there, Miriam, is we've recently moved our financial data from an Amazon Web server in Dublin, UH hosted cloud AWS to Azure Active Directory via Dynamics 365.

22:23  
And as part of that procedure, we now backup the data via immutable backups.

22:27  
So what that means is that every 12 hours it creates a backup and nobody can ever touch that data.

22:32  
There's a full log of what's going on.

22:34  
Like that.

22:35  
Again, is in terms of encryption, but do companies know that that's available or what it does or whatnot?

22:41  
I I think just maybe just have a look at question 22 because again, similar to what you were doing in 21, I know exactly what you're trying to ask, but I would just be worried that everyone's just going to click the first option and it's not going to be a worthwhile question because they're just going to have 100% of people answering the first one.

22:55  
Do you get where I'm coming from?

22:56  
Yeah, no, I do.

22:56  
Yeah, brilliant.

22:59  
Do customer, do you process customer payments over the phone?

23:01  
No, it's all via IPEN and whatnot.

23:04  
Do you share customer data with third parties, EG delivery drivers, not directly hire with you outsourced?

23:11  
That is a good question.

23:13  
Again, there's a lot to it.

23:16  
I mean, I would say yes, as much as they need to complete their job.

23:19  
An example being is we have a pharmaceutical project.

23:23  
We have 350 people in Blairney at the moment working on it.

23:26  
So of course, there's going to be design coordinators and engineer consultants and whatnot.

23:30  
We're going to be sharing not just customer data, but personal data as well, trying to get everybody.

23:35  
But it's all done specifically in Procore so that there's all logs and data of it or whatnot as well.

23:41  
I I think it's actually a really good question though, because so like there might be a question on it as well.

23:47  
But we as part of our cyber insurance renewal, we've just finished cybersecurity training on all of our staff and whatnot.

23:54  
And as part of this, this was actually a kind of a module on it that I had created is not giving people full access to things, only give as much as you need, you know, granular permissions.

24:04  
Do they need to be able to view and download everything or can they just view what's needed and not actually extract the data?

24:10  
So I think it's actually a good question because, umm, it'll be interesting to see if people just, you know, I'd say a lot of people just click the middle one anyway, but umm, I'd say there are quite a lot of businesses out there because I've seen them myself that like, oh, I'll just share that with Miriam.

24:22  
And they don't even look at the permissions.

24:23  
They're just going to type in your e-mail and just share with you.

24:25  
And umm, I've even gotten access to things that I shouldn't have, not at Seafield, but at other companies have had to ring them and be like guys.

24:31  
I only need to see, you know, whatever it is and what not.

24:33  
So, umm, I think that's a that's a very good question.

24:36  
Umm, backups.

24:37  
So again, umm, automated.

24:39  
Umm, I think there might be a fourth answer there.

24:43  
I perform both automated and manual backups because there are companies that do that.

24:48  
Umm, if there was an option there, I would do it as well.

24:50  
The reasoning being is all of our backups are automated.

24:53  
That's fine, but there are certain times when you need to do manual ones.

24:56  
Umm, if you're doing like a big update on a server and you want to just create a quick backup just at that moment in time before you do it, umm you know bits and pieces like that.

25:04  
So I think it might be worth just maybe having a second option.

25:06  
Umm in between.

25:07  
Just saying I actually do manual and and automated backups.

25:10  
Umm because uh, some companies do that as well.

25:13  
Umm how often do you complete the backups?

25:15  
Umm again, this is a loaded questionnaire.

25:18  
What I mean by that is like we probably have 7 to 10 backups at any given time, but some of them are weekly and some of them are daily.

25:26  
Maybe just specify like how often you're going to complete maybe critical data backups, maybe even just putting the word critical in there, because if that's the case, I'd argue daily.

25:35  
The only ones that I'm really seeing weekly are I actually, I can't even think off the top of my head a weekly backup, but we probably have one or two of them.

25:43  
But I'd say a lot of the core data that we were talking about there pro core, Dropbox website, financial data, all that stuff, not even daily.

25:51  
It's probably every 12 hours.

25:52  
It's probably twice daily just to make sure we have it.

25:55  
But again maybe just maybe just put in the word critical just so people understand kind of what's what's being asked there.

26:01  
Oh brilliant.

26:02  
Here we go 27 immutable aircraft backups.

26:04  
That's fantastic.

26:05  
You're keeping tight like about that.

26:06  
That's brilliant.

26:08  
That's exactly what we're we're looking for there.

26:11  
So yeah, exactly just for from my from my thing there.

26:14  
So that was a big thing for us when we were looking at our financial data is just making sure that umm and a again, I don't know if you want to either put in that question as a follow up, umm like is there a log kept of these backups or is there uh like a a formal structure kept.

26:29  
So as part of our disaster recovery plan or DRP we have to have a log in place that like if Miriam goes in before backup is done and changes something, do I have a log Because immutable means that it it's changed.

26:40  
Umm like, uh what?

26:42  
What?

26:42  
What's called after?

26:43  
And rest, which means like it backed up and then it's in a server, but before that backup you can do whatever you want to it.

26:49  
So is there a log beforehand?

26:51  
So I think again, it's only just for yourself.

26:53  
I'm not, you know, saying what to do.

26:54  
I think it's a great question.

26:55  
Anyway.

26:56  
Umm, I'll be very interested to see.

26:58  
Umm I suppose the answers if people even just even know what an immutable air gap backup is because I think that would be good.

27:04  
Umm.

27:05  
Or is is tested on a a biannual basis.

27:08  
I don't know if there's I know I'm getting awkward with the things I'm just going to do annually just for the sake of it anyway.

27:13  
But umm I think like I think some people do monthly ones and I'm like I suppose we probably should do it a bit more often.

27:21  
But as I said there's only two of us and 185 employees.

27:24  
So I I think we're we're we were doing well that we have backups in the 1st place.

27:28  
Umm, but umm you'll see yourself Miriam, umm as part of cybersecurity, umm insurance and whatnot.

27:34  
Not you have to have a disaster recovery plan and you have to have a log in terms of when you're doing backups, have they been tested and and so on And some of them, like I will say this, sometimes testing backups is either very difficult or impossible.

27:47  
Like our financial data would be very difficult to test if the backup works because like they're working on it consistently.

27:54  
It's not a case that we can just put it back into the server.

27:57  
Like it's a little bit different with maybe a Dropbox folder that you can restore to a different place.

28:01  
Now maybe that's just, you know, me being an IT manager and and whatnot as well.

28:06  
But I think definitely it's a, it's a great question because some people will literally click this.

28:11  
I've tested it once and I think it's working fine, which is that's where I start to lose sleep if if that happens, do you follow the role of access control?

28:20  
Yes, exactly.

28:21  
So that, that again, that's what we were chatting about earlier.

28:23  
Miriam is a great question.

28:24  
There is that, you know, do they have it for things?

28:27  
I think a lot of people, they probably do this, but they won't click on this.

28:30  
Is that somewhat, umm, I I think, umm, that's what our training tried to focus on from cybersecurity is that everybody has a responsibility that when they're sharing things to make sure that they're looking at it like it's not just the directors of the IT department, It could even just be the accounts team.

28:44  
Like are you giving people access to things that they they shouldn't be seeing?

28:48  
Umm.

28:48  
So every every year now we're going to have a refresher on that just to make sure that they know what's what's going on because umm, unfortunately, things change the, the layout changes, UI changes.

28:58  
You know, sometimes you know that you're giving people only certain permissions and then IT changes, uh, you know, that kind of way.

29:03  
So umm, who has admin permissions?

29:05  
So the only people that have it is the IT team.

29:08  
That's it.

29:08  
Now a great, umm, follow up here, right?

29:11  
Admin privileges is a very catch all term.

29:14  
So to put into perspective Microsoft admin lists, I'll actually show you for a second, one second now because I don't think there's anything in here untoward.

29:23  
So this is just our Active Directory, this is just where we, but if I go to umm, roles for a second, right.

29:31  
So these are all the different roles that are considered administrators in, in the sense like.

29:37  
So what you're probably asking for is maybe global admin, which is access to everything.

29:42  
I would maybe be just a bit more specific on what admin privileges mean because in an IT sense they could mean loads of different things from are you just managing Microsoft Teams to are you the users, are you managing whatnot as well?

29:55  
Now again, similar to what I was saying, I understand exactly what you're asking for in the question.

29:58  
Like you know, do people who aren't supposed to be admins have admin privileges?

30:02  
But maybe just, uh umm just maybe explain a little bit more what admin privileges you're actually looking for.

30:08  
Like, is it global admin, is it managing users?

30:11  
Is it what?

30:12  
Not as well?

30:13  
Umm, but regardless, anyway, it's all the IT team.

30:15  
Now you could argue there's one or two directors who have admin privileges for Dropbox from document standpoint, but again, that's not really cyber security as such as they still have all their MFA and everything.

30:24  
I think what you're probably meaning there.

30:26  
And again, uh, I can see in your thing installing software, configuration changes and whatnot, that's, that's just the IT team MFA.

30:34  
Yes, exactly.

30:35  
For all items.

30:36  
Oh, I was just going to say a question should be on what type of MFA.

30:39  
Brilliant.

30:40  
That's.

30:40  
And again, that's what we're talking about there.

30:42  
So we have authenticator app, we have SMS code.

30:49  
What does code mean in this instance, Miriam?

30:52  
Yeah, we were.

30:53  
So like for me now I have and when I try to log into my e-mail on my laptop it will send me a code to my actual e-mail app.

31:03  
OK, So what I would do is I'd probably just put an e-mail instead of code maybe just because like the argument being is that they're probably all codes as such if you get me.

31:13  
So I'd probably just put e-mail in there just to see.

31:15  
So for us anyways, they're saying SMS and I suppose you can imagine construction.

31:20  
Most people are SMS.

31:22  
Still.

31:22  
I'm slowly trying to move them over to Authenticator app, but it's a a big thing and you might have seen this as well, is that we actually didn't use Authenticator apps for a long time.

31:30  
And I don't know did I mention this last year in our last meeting.

31:32  
But they were susceptible to brute force attacks.

31:34  
So you'd keep pinging the app until the person was like oh just go away, I'm just going to click confirm and it would leave them into the e-mail address.

31:41  
So you've probably noticed on the new Microsoft one and whatnot you have to type in a code still, but it's like a 2 digit one, like 76 that's the stop brute force attacks so that somebody has to actually action what's going on as well.

31:52  
So now that we know that that's been implemented, it's, I know it's been about a year or whatnot, we're slowly migrating everybody over to authenticator apps because SMS are still not as not as secure as they need to be.

32:02  
So that's fine.

32:03  
This was again fantastic question.

32:05  
We literally had a whole module on this on our cybersecurity training is, you know, Jim is in the accounts team and he forgot his work laptop.

32:12  
Can I borrow your credentials to log in for the day?

32:15  
Literally something.

32:16  
Is that.

32:17  
So the answer is yes.

32:20  
Some passwords are shared, though unfortunately is I I have to be honest.

32:23  
Umm, at the moment, Umm, there's one single password that's shared.

32:27  
So when you have a C field device, umm, we have a Gmail account to allow you access to the App Store for our particular work apps and whatnot.

32:35  
Umm, we need to upgrade it.

32:37  
It's called Android Enterprise.

32:38  
It's it's a big undertaking or we just haven't at the time at the moment.

32:41  
So literally all we have is a Gmail account and a password to log people in.

32:45  
It's it's not the most beautiful thing and I know from a security standpoint, Now security standpoint, there's nothing in it except for apps download and whatnot.

32:52  
There's nobody's details in it or anything like that.

32:54  
But still, I have to be honest and say yes, some one password is shared if I if I even had an answer to that.

32:59  
But do you require staff person to have minimum length?

33:03  
So great question, yes.

33:05  
But software enforces this.

33:07  
So we use the Microsoft standard, which I believe is 8 digits alphanumeric and there has to be one capital letter.

33:17  
And I don't think we do the the special character.

33:20  
Like we kind of joke that you know it's gotten so bad that you need to put in hieroglyphics or do you know Chinese symbols or whatnot to try and get it.

33:27  
It's gotten really bad.

33:30  
I think now I don't know if it's.

33:31  
I'm going to just sneak past here for a second and just see umm.

33:34  
I think a really good question on this Miriam is umm, and I definitely think it should be a 35 is how often are these passwords changed or reset or something to that thing.

33:45  
And the reason being is it's a false question.

33:48  
So as of a a year, a year and a half ago, the recommendation from cybersecurity is you should never reset or set as you probably know yourself, from talking to somebody that knows exactly.

33:59  
And the reasoning being is it ends up being June 1, June 2, June 3, and by the end of it, you can't remember what password you have and whatnot as well.

34:06  
Umm.

34:07  
So I think that might be a nice question because I'd say a lot of people are very similar.

34:10  
And what's really frustrating is like I'm dealing with some of the biggest businesses, uh, BT, British Telecom over in, umm, England.

34:16  
We have a corporate account with them.

34:18  
Every 90 days I have to change my password to their admin center, which is just ridiculous.

34:22  
And I'm, I'd say I'm on about the 7th!

34:25  
Of the same passage that I've been using just because I can't be be dealing with it.

34:29  
You know, I see you have a passive manager.

34:30  
A question there.

34:31  
Yeah, we use passive managers still.

34:32  
But I think that would be a great question just to say.

34:36  
Umm and I would probably phrased it as a trick question saying how often do you reset it and you could have never.

34:41  
You could have three months or whatnot as well.

34:42  
And I'd be really interested again just to see umm where they're at because umm like even for the cybersecurity insurance again to come back to it, they they asked that question specifically.

34:51  
Do you know do you have it thinking that you should know the answer is actually no you shouldn't.

34:55  
They you know it's only as as as ha ad Hock and as an is so umm I just said I'd say that to you anyway and password manager.

35:01  
So great question right.

35:03  
Some staff.

35:04  
Umm and the reason being is they're still not as prevalent as you'd as you'd like them to be.

35:10  
Umm they're still more IT niche.

35:12  
Umm I would love people to I mean you should see I'm not going to name names obviously on a recorded call but some of the lads literally have spreadsheets of dozens of passwords to everything from their bank accounts.

35:22  
They're thinking I'm like lads please I mean you can't be doing that.

35:25  
So again, as part of the cyber security training, I think this is a great question.

35:29  
We went through password managers, we went through, umm, encrypting Usbs.

35:34  
We went through just all that kind of stuff, uh, putting like a very simple thing, putting a password on an Excel sheet before you send it if you don't want people to see it.

35:40  
And like people found that very, very, uh, you know, responsive.

35:44  
So some staff is going to be the answer.

35:46  
You know, I I would know off the top of my head a lot of people are.

35:48  
But umm, I I don't think I would be very, very surprised if someone said yes, all staff because umm, like even directors, I'd say a lot of the time they don't even know that they're doing it.

35:57  
I know you could I argue and you know what's actually a very fairpoint, you know, it is a password manager.

36:04  
You know when you're like saving things to Chrome or whatnot and it says would you like to save this password to it.

36:09  
That is a form of password management and it was something that we were looking at.

36:12  
So I mean the answer maybe would be yes, but I I would probably look at it in the traditional sense of do they actually have a a password manager that they can they can do is all.

36:20  
I'm just saying there, umm, you enforce block listing passwords.

36:23  
Umm.

36:23  
So again software configures that.

36:25  
So again we use the Microsoft default.

36:27  
So you can't be using things like password or your name or your location or things like that as well.

36:32  
Umm, they have like a a block list that they update I think every, every month or something like that.

36:37  
So Umm, yeah, very, very similar to that.

36:39  
We we'd use Microsoft's default there.

36:41  
Umm, how often do you and your employees engage in cyber security training?

36:44  
This is great.

36:45  
We uh as as recommended by the UH the insurance company once a year.

36:50  
So the the reasoning being is that you only need to have a full formal training session for UMM.

36:56  
They didn't really say a minimum of an hour but they do recommend 60 minutes or as was 88 minutes long.

37:01  
It had 13 modules.

37:02  
It spanned loads of different things we were chatting about earlier.

37:05  
Um.

37:05  
And then the recommendation is that you have refresher courses then every year for about 20 or 25 minutes just on what came up throughout the year.

37:12  
So is there, um, you know, an increase in phishing emails?

37:15  
Is there an increase in whatever the case may be?

37:18  
Um, like you know maybe two years ago there would have been a big thing on ransomware and all that kind of stuff as well.

37:23  
So that's what we're doing at the moment.

37:25  
So we're we're rolling that out.

37:27  
I think the the big issue if you ever want to report back is if anybody knows how to get everybody to do their cybersecurity training.

37:34  
That would be a fantastic company to work with.

37:37  
We managed to do well.

37:38  
We got you know a a good chunk of people to to do their training anyway and we'll we'll keep at them until they do it.

37:43  
And what methods of cybersecurity training have you or your staff undertaken?

37:47  
So, right you again, I'm going to tell you what we've done and you might let me know if there's an answer for it or do you know or whatnot standard in corporate industry and I'm talking they were like 200 employees like we have or whatnot.

38:03  
We outsource the development to a company.

38:07  
So in this time, it's an Irish company called Infosec and they basically have a Bank of thousands of modules to choose from and you then create your own video presentation in it and you send it out to staff.

38:18  
But more importantly and specifically where we went with Infosec, uh, Miriam, is because it's fully, umm like, uh, you have to be in there.

38:26  
So what I mean is like the first section is about phishing emails.

38:29  
Once the videos are played and whatnot, they will actually show you a physical representation of an Outlook mailbox and you have to choose the different phishing emails.

38:37  
So it's not just sitting in front of a thing like we're getting people to do this stuff like interactive is the word I'm looking for.

38:42  
So I I don't know if it answers any of yours or if you were to say maybe to be like an interactive course, you know where I'm coming from there.

38:51  
Yeah, no, I do.

38:52  
Maybe if you could you type the name of them into the other.

38:55  
Yeah.

38:55  
So like, it's literally just called infosec.

38:58  
But like, I'll just show you, I'm just going to stop sharing this for two seconds and I'm just going to see, can I can I bring in?

39:04  
Because I don't want to show you certain information, but if I can, just just to give you an example because again, like, I just think it's frustrating from your point of view that you don't get to see a lot of the corporate, you know, aspects of what people are actually using.

39:16  
So I just want to show you what we have.

39:22  
Here we go.

39:22  
Brilliant.

39:23  
OK.

39:23  
So can I?

39:26  
Yeah.

39:26  
I think I can just do something like this for a moment just to show you.

39:28  
You know, it's only just So this is the Infosec platform.

39:31  
OK.

39:32  
So this is like my admin panel.

39:34  
So this is the training that we're doing.

39:36  
So we had 170 people doing their cybersecurity training.

39:39  
So you can kind of click in and you can actually see all the different modules that they had to do.

39:43  
So we now we spent weeks setting this this up so you can see the the heading of it like social engineering.

39:49  
Now that's actually a really good one that we haven't talked about as well you know all that kind of carry on and so inside it then as well what there was is there was videos there was quizzes, there was interactive stuff and what not as well.

39:59  
So this is just one of the platforms.

40:01  
So I just put in Infosec there just so you can have a look yourself and see.

40:05  
But I I don't know if you want to put in an answer saying maybe like.

40:09  
I don't know third party services or whatnot because like technically we didn't do the cybersecurity, we put them onto the platform.

40:16  
But as an IT department, we still had to create the thing.

40:19  
We had to make sure that it was for C field staff and whatnot.

40:21  
Umm, so it's up to yourself.

40:22  
Any whatever you think would be would be best on that.

40:25  
Umm, yes, that's a a huge thing.

40:27  
Again love to see the answers on this as well.

40:30  
Like that's a a huge thing.

40:31  
We we have a really clear procedure on if you've gotten a phishing e-mail or a spam e-mail, get onto myself and Kahul, disregard, delete it.

40:40  
Don't click on links.

40:42  
A huge thing in the cybersecurity training.

40:44  
You know hovering over a link shows the correct URL.

40:47  
How people can hide hyperlinks and different things like that was a a really big part of it as well.

40:52  
So I think that's a fantastic question if a cyber incident occurs, OK, so that is a great question.

41:00  
I'm going to have to answer the second option, although I'd like to say the first.

41:04  
The reason being is that it will be very difficult to have everybody knowledgeable on the DA disaster recovery plan, umm, which which includes cyber security.

41:14  
And I think and that's that's a cop out for me because really the answer should be #1 that all staff are aware.

41:19  
But like I just, I can't see a site manager or a foreman or whatnot even understanding like they're they're very good that they'll give me a call and say look Ross, something has happened or whatnot as well.

41:29  
But the reason that I'm saying some staff is that in a disaster recovery plan you have to umm like mention certain people and whose role is what?

41:37  
Like there's no way that you're going to be mentioning 170 people and Miriam is going to be doing this.

41:42  
If she do, You know what I mean?

41:43  
It's a cork amount of people.

41:44  
So again, I'd love to see the answers.

41:46  
I think that's the reason that I'm choosing the the second option is because that's what we went with in terms of it.

41:51  
Umm.

41:51  
And then yes, this is it.

41:53  
So again I it's tested regularly and updated.

41:56  
I'd maybe go a bit further and similar to your other question, how regularly is or is a test and updated?

42:02  
I I think it's a bit of a broad one there.

42:04  
Again, is it annually, is it biannually, is it whatnot as well, Umm again to come back to the cybersecurity insurance or it has to be tested at least annually and it it there has to be a umm an evidence log of somebody looking at it if there's any amendments done or things like that as well.

42:19  
So we do that as we're applying for cybersecurity every year and it just reminds me okay, let me just edit it.

42:25  
And like usually once you have it created like it's a big long document, there's not much that changes unless there's new IT services and support goes in and whatnot as well.

42:34  
But yeah I just said and then in including that then as well.

42:37  
So or like these are really good questions because I actually had to look up the difference between an incident response plan and a continuity plan when I was doing the the thing.

42:47  
So what I did was I just created a disaster recovery plan in DRP which included all of these as as standard and it just kind of fitted the bill a little bit more.

42:56  
So again I I would you know consider those to be one of the same but I still think it's a great that you've listed it out because I didn't even know.

43:02  
I still a little bit unsure and I'm the IT manager.

43:05  
So for now I've just put everything under the disaster recovery and what not as well and I think that's everything.

43:10  
Is it?

43:11  
Yeah.

43:11  
If you just press next.

43:13  
Yeah.

43:14  
All brilliant.

43:14  
And there's a few others brilliant.

43:15  
This is just the feedback partners that's the yeah, like, I think it's they're they're great, very clear and concise and that was very good tool was very easy to use.

43:28  
Of course, Microsoft Forms is always brilliant, Very easy to use and navigate.

43:38  
Yeah, hugely relevant to the business, hugely relevant to any business really.

43:47  
I'd say.

43:48  
I mean Jesus, not just us here and any business.

43:52  
And very beneficial exercise, very beneficial exercise, umm, feedback.

44:06  
I'll, I'll leave that for like I'll just leave that as a dot because obviously this is probably the feedback that I'm presenting here at the moment.

44:12  
Umm, so I'm just going to submit that.

44:13  
And now I have a meeting at 4:00, but if you have 10 minutes, I just want to go through a few things that I think would just be very handy for you, if that's OK.

44:20  
So the first thing is and I don't know again if umm, like this is literally, I mean your ears must be burning because this is something that that was it was actually part of a a tender for a client.

44:31  
Obviously I can't say who it was that they were looking for this certification and it's something that we have to go towards, but umm, if you give me a second, I'm going to find the e-mail that I'd sent to one of my contacts just in relation to it.

44:45  
Umm, here it is and I just want to show it to you because it's it's becoming very relevant.

44:52  
So I'll what I'll do is I'll, I'll send you this link just so you can have a quick look.

44:55  
Now, don't mind how busy it is and everything, but basically this, umm, you're probably aware, aware of the ISO kind of things and whatnot as well.

45:03  
This one is becoming hugely important and it was only, umm, finalized, not even 2022, I'd say maybe 2023.

45:10  
Really.

45:11  
It's the information Security Service, security and and privacy protection for all management systems.

45:16  
So it's document management systems, data management systems and whatnot as well.

45:20  
It's something that we as a business are going to try and get towards because a it just saves me a huge amount of time having to list everything that we do with the business.

45:27  
Basically you just send them the certificate and you say, OK, we know what we're doing.

45:30  
But second of all, it kind of gives me a checklist of am I doing things correctly as a, you know, IT manager.

45:36  
Second, but as a cybersecurity expert, really, first of all, umm, so I only just said I'd mention to you because I think it might be worthwhile just to not even, umm, you know, delve into it because there's like ridiculous amount of pages in it.

45:48  
But maybe just like, is there going to be a question on the thing you know?

45:51  
Are you aware of this ISO?

45:53  
Umm, is there something that you're working towards or what not?

45:55  
Because I'll say I'll know to both them.

45:57  
I wasn't aware that it was here and neither did I realize how important it was.

46:01  
But you're starting to see now a lot of businesses especially clients that we deal with which would be actually manufacturing and construction and whatnot and pharmaceutical.

46:09  
These are the things that they look at in terms of are you going to win the tender or not.

46:13  
Like everyone can say oh we're up to date and security we we patch all of our windows things.

46:17  
But having this means that we've we've really done our due diligence and we've gone through.

46:21  
So I only just wanted to show you that first of all because that's actually something that we're we're going through as of this week.

46:26  
I have a meeting with them next week just to kind of formally start it and see what's needed.

46:31  
So that's one thing.

46:32  
And then I just want to try and see can I show you an example of a of a cyber security form or a cyber insurance form, just to kind of give you an idea of just how insane the questions are, like not from a bad, like I think they're great, but I just want to make sure that there's.

46:56  
Yeah, I see this one is answered one second.

46:58  
Now I want to see the if I can get one that isn't.

47:02  
Do you know what she might have sent it to me without Sorry, no I didn't actually think that I was going to be doing this.

47:13  
But I just think it's just definitely worthwhile for do do do here we go cyber liability.

47:24  
See, these are quotes.

47:32  
OK, so this is like one example.

47:36  
OK, so I'll show you that in a second.

47:37  
I'll.

47:37  
I'll bring that up in a moment.

47:38  
I just want to show you the actual document just to give you an idea of, OK, here, here we go.

47:48  
Right.

47:48  
So this is, this is actually a supplemental.

47:52  
So this isn't even the main one, but this is the only one that I can find.

47:54  
I don't want to be, you know, keeping you waiting, but this is just one that we haven't filled out.

47:59  
This was actually supplemental to the other 31 pages.

48:02  
But just to give you an example of the the amount of data that they look for.

48:06  
So this is just purely ransomware and like what's the other one and like identity and access management and whatnot.

48:15  
So you could just see like they look for like how much you spend on an annual basis, like all the very specific things that you're doing like e-mail security, are you tagging external emails?

48:26  
Like how is your UH demark, DKM and SPF records, which has actually become a huge item.

48:30  
Umm, now that some third parties are UMM, there was a big item from at the start of the week from Microsoft, Umm about it.

48:37  
Like how you like?

48:38  
And then do you require additional training for employees who fail phishing simulations?

48:41  
So it's not even there.

48:42  
They're already presuming that you're already doing the simulations.

48:45  
Like, what do you do if somebody fails it?

48:46  
Like very specifically, what licenses do you have?

48:49  
Because then that'll tell them you know what cybersecurity have for it as well.

48:53  
So like what I'll do is I'll send this on to you I have no issue and it like it's not a it's just a document that you've you can if get online anyway if you're going through them but but I'll I'll send that to you just because and like this is again a supplemental this isn't even the main body of the cybersecurity insurance it's like 31 pages normally.

49:10  
So it's it's kind of crazy in terms of what's needed for for that.

49:14  
And then I think this is the the other one, right.

49:16  
So this is the terms and conditions then for all of your cybersecurity insurance.

49:22  
So this is like what we have to agree to before we're even able to like it is all the subsections and everything like that.

49:28  
Is that like you can just see it's 18 pages and like that that's after we fi fill out the 31 pages.

49:33  
So I'll, I'll send you both of those.

49:34  
Again, I I don't think there's any issue with me sending them on because they're just, they're just, you know, wording and whatnot as well.

49:39  
But just to give you an example of, umm of, you know, I suppose how stringent they are really at the moment.

49:45  
And I think, I mean if you're asking me, I, I think it's a bit, umm, annoying, not from us because we're doing very well, but like if you're an SME, you want cybersecurity insurance because you're worried about it, but there's absolutely no way that you're going to be doing everything if you have 20 employees.

50:01  
And John is the managing director, but he's also IT part time on on the side, you know, like it, it's just not going to be happening.

50:07  
And I think it's really frustrating because like it's very obvious from my point of view from a, from professional standpoint that they're only going to be maturing the companies that are probably not going to be hacked in the 1st place or going to have very low, you know, aside from it.

50:19  
Like I mean again Touchwood, you know, I I hope it doesn't happen with us, but umm, I just wanted to show you that anyway from a context.

50:25  
So I'll send that on as well just to make sure that you're kind of aware of it and.

50:29  
But is that OK?

50:29  
Anyway, do you have any questions or queries before I leave you going finger just to thank you because it's good to hear from someone you know.

50:36  
Obviously you have like umm background in it and stuff and that you're managing a bigger company because people we have been talking to are like you know, five employees are just themselves.

50:45  
So it's such a different, umm experience then to have someone who has much dealing with much more people.

50:52  
So that's really insightful.

50:54  
It's really useful.

50:55  
Thank you.

50:55  
No problem.

50:56  
And like as I said, look don't be a stranger.

50:57  
I think as I said to you last year, MTU was was great to me when I was doing my masters.

51:01  
I thought they were fantastic, all the lectures and everything like that as well.

51:04  
So if there's anything else, any kind of follow-ups or anything just let me know.

51:08  
Like I'm always usually free for 1015 minutes if there needs to be another call or anything like that Miriam.

51:12  
But umm, look, as I said, best look again and umm, I don't know if you're allowed to share the results anonymously or whatnot, but I'd be really interested to see, do you know some of the even just the the questions that I highlighted there because umm, I just think it's one of those areas.

51:25  
Umm, and I suppose I'll end it on this is that, umm, if somebody types in cybersecurity into Google or I'm looking for help with cybersecurity, you've all these multibillion dollar companies that are willing to help you, but like, they'll charge you an arm and a leg and you know, uh, you don't really know unless you're someone like me cutting through the weeds.

51:45  
Do you actually need all this or are they just trying to upsell you or whatnot?

51:48  
Umm, and I think it's really frustrating because there's nothing really out there at the moment.

51:52  
And that's why I really love the idea of your tool.

51:54  
Just to see a again, it's from a resiliency standpoint, a checklist.

51:58  
Are we doing just even the bare minimum?

52:00  
Like, I mean the amount of people that don't even know what MFA stands for or what it's needed.

52:04  
And like we even when we brought into the company, when I first started, there was people sighing and oh, why do I have to put in a code every time and whatnot?

52:11  
And now it's become so.

52:12  
So part of it that if we're dealing with subcontractors specifically on site and they don't have it, that's like the biggest red flag, like it's like, all right, we're stopping everything.

52:20  
Can we have your SEC.

52:21  
Security insurances?

52:22  
How are you doing IT?

52:23  
Because that's like such a a blatant disregard to security that you don't even even have it on it.

52:28  
But yeah, as I said, I like, you know, probably every day website, probably 3035 people are trying to get hacked and I'd say at least 100 attempts every day on an e-mail address in sea field, if not more.

52:42  
Umm, like I I could show you it for hours, like all the different countries that are trying to to try it and whatnot.

52:47  
Umm, And sometimes, like I say to the lads, umm, you know, don't worry if someone gets their password, obviously it's really bad, let me know, but it's not going to be the end of the world, right?

52:54  
Because they don't have your code, they don't have your tokens and whatnot as well.

52:58  
The only thing that I'd be annoyed with is that we give everybody a password when they start and we say, look, you're more than welcome to change it, just don't change it to something that you already know.

53:05  
And I'll be chatting to someone and say, oh that's my banking password as well.

53:07  
I better change that.

53:08  
And I'm like, don't tell me it's your banking password, please.

53:10  
I never need to know that.

53:12  
So we'll we'll see how we go anyway.

53:14  
But look, I got a headway, Miriam.

53:15  
I'll.

53:15  
I'll send you those before I head to site.

53:17  
Anyway, before I forget.

53:18  
And as I said, if there's any questions or queries, just let me know.

53:21  
All right.

53:21  
Thanks so much, Ross.

53:22  
Thanks.

53:22  
All right.

53:23  
God, have a good evening.

53:24  
Bye, Miriam.

53:24  
All the best.

53:25  
Take care.

53:25  
Bye.

53:25  
Bye.