**Risk Assessment Tool Pilot - Sine-20240403\_090346-Meeting Recording**

0:02  
More options here or, you know, anything that comes to mind just so we can edit it and stuff.

0:09  
Yeah, yeah, yeah, no problem.

0:29  
And about how long will it take to run through?

0:33  
It takes about anywhere between 5 and 15 minutes.

0:39  
OK, so it's not too long.

0:41  
So did the e-mail send?

0:44  
Oh, e-mail.

0:44  
Sorry.

0:44  
I was looking at chat.

0:46  
Awesome.

0:53  
Yeah, great.

0:56  
OK.

0:57  
So risk assessment, consent.

1:00  
Yeah.

1:01  
Just like I don't know what MTU is or I don't know.

1:04  
So just put it in, I suppose somewhere.

1:06  
And that's why I was asking just for a quick overview and that in any sort of form.

1:11  
I just, yeah, OK.

1:14  
I've read the instructions.

1:21  
I haven't read the instructions.

1:23  
Yeah.

1:23  
So it's attached there.

1:25  
So I have to read that.

1:26  
OK.

1:37  
OK.

1:47  
Did you give me this letter before?

1:49  
No, no.

1:50  
OK.

1:59  
OK, great.

2:06  
OK.

2:09  
I have the opportunity to ask questions.

2:10  
OK.

2:11  
Yes.

2:13  
Great.

2:18  
No, I'm a limited company.

2:19  
Is that OK?

2:20  
Yeah, that's fine.

2:32  
We're like sort of more in Wellness, but I'll put healthcare.

2:40  
So in terms of cybersecurity.

2:42  
So what I do is like, every so often I get someone to help.

2:47  
OK, yeah, I don't have anyone.

2:49  
So is that an outsourced person?

2:51  
But it's not like a constant.

2:53  
It's not someone all the time.

2:54  
So maybe it's other ad hoc that's actually good to know because I'll add that in as an option.

3:02  
Yeah, like I said, I'm a small company, so I just maybe at the beginning, you know, I got someone to assess it and then every so often I would, yeah, it's cyber insurance.

3:12  
Gosh, so I've public liability insurance.

3:16  
I've published insurance.

3:17  
Is this like from a cyber attack?

3:21  
Yeah.

3:21  
So it'd be specific to cyber itself.

3:26  
Yeah, like, I suppose.

3:28  
I suppose.

3:29  
I'm not sure.

3:30  
Just so you want me to think out loud, this is what's going through.

3:33  
My head would help If I protect me.

3:37  
I don't have anyone's credit card data.

3:39  
I have.

3:40  
Yep, all the product, liability, insurance, and professional indemnity.

3:46  
But I I suppose Register 365 might protect me a little bit on things as well.

3:53  
Yeah.

3:54  
OK, we'll keep finished that.

3:57  
OK.

4:00  
Yes, Third party.

4:06  
How is it managed?

4:14  
So it was set up by a third party specialist, but it's not regularly maintained by them?

4:19  
Yes.

4:20  
Do you feel confident?

4:21  
No.

4:22  
Which is why I'm doing this.

4:24  
Definitely.

4:25  
I'm doing it so when people are like all my suppliers use their own work computers and everything.

5:04  
And I I use like a phone and a laptop.

5:07  
So is that members of staff using personal?

5:10  
I suppose it is not really.

5:12  
So a personal company computer and it's a company phone.

5:15  
Yeah.

5:16  
So a personal phone would be like your phone that you.

5:19  
Yeah.

5:20  
Just for your personal use.

5:21  
Like would you use that then for business emails and stuff?

5:24  
I don't have dual phones.

5:26  
Yeah.

5:26  
Yeah.

5:26  
So yeah, that would be, yes, antivirus on your devices.

5:34  
Do I have antivirus?

5:43  
I don't know, like Android sort of is really good.

5:46  
Like I don't know you had to buy an antivirus for Android and Mac as well.

5:53  
Yeah, because I know some of the Android phones, they have antivirus just built into the model.

5:58  
So I have a Pixel, so it's literally, I don't see the need.

6:03  
So it's more that I yes, I would say do I have a specific one on my Mac?

6:11  
Again no.

6:12  
But I I have Parallels Desktop as well so I can duel I can have a like a another desktop if I need it and there's antivirus on that.

6:24  
So I don't know.

6:26  
I don't have a separate Mac one though.

6:28  
Maybe on some some devices, yes on some.

6:32  
But I'd actually add another option into that to say that it's automatically on.

6:38  
Yeah, I think you should just have other and a few of these you'll get.

6:41  
Yeah, yeah, yeah.

6:43  
Do you have spam filters?

6:44  
Yeah.

6:46  
Are work devices wiped?

6:49  
Yeah.

6:51  
I have not needed to this yet.

6:56  
It's all automatic.

7:02  
OK, so if I do ever do a payment over the phone, it's actually me or someone working with me doing it through the back end on Shopify.

7:39  
So we we put the data into the system, but it's automatically deleted.

7:46  
Any credit card data is automatically gone into the system automatically on it like it's never saved.

7:51  
Yeah, that's.

7:52  
That's perfect.

7:53  
Because the question after, if you say yes to that, it will give you options to.

7:59  
OK, perfect.

8:00  
Yeah.

8:02  
It's inputted.

8:03  
Yeah.

8:03  
Perfect.

8:04  
So it's not.

8:06  
So is that the data is inputted directly into the payment device.

8:08  
Yeah, yeah, yeah.

8:10  
We don't store it customer data.

8:15  
So we share like DPD would have access to addresses.

8:19  
Yeah, there was that.

8:23  
So that would be as much as they need to complete.

8:28  
Yeah.

8:32  
OK, I'm not sure.

8:36  
OK.

8:43  
And here, so there's no need for this for which question, Immutable or air gapped backups from our business critical data.

8:51  
So I don't need that for my business.

8:54  
OK, perfect.

8:56  
So it's not that I don't, I don't have it.

9:01  
Yeah, if you want to say, I'm not sure on it and then I'll add in.

9:06  
Yeah option.

9:08  
OK.

9:22  
So I do work with third party suppliers obviously.

9:25  
So to do with them marketing or SEO or any of like website updates and I would only ever give really strict permissions in terms of access.

9:37  
So.

9:39  
So I think the the word staff is probably incorrect there because they're definitely not staff.

9:45  
Yeah.

9:46  
So it's it's where staffers, third party suppliers basically just.

9:57  
Yeah.

9:57  
Yeah, perfect.

9:58  
Thanks.

9:59  
Just wait on that Tim.

10:00  
Yeah.

10:01  
So I'm just writing.

10:02  
Yeah.

10:02  
Or they have access to what only what they need which is how I how we approach it for anyone, anyone working with us.

10:14  
So sometimes again admin privileges, they're very that's that's quite a blanket statement but there'll be admin needs for really different things So, so say with like Facebook, certain people would need admin rights but they wouldn't give them rights to like TikTok or Instagram or something else where they only wouldn't have admin rights to Shopify, do you know what I mean?

10:35  
So that's probably a bit blanket, yeah.

10:40  
So like an outsourced third party doesn't have like admin privileges but it's more that's where where required.

10:48  
So some like it says installing software, so some say with Shopify you have to install new updates to your template.

10:56  
So I would, there's a company in Mayo that we use and they have to have admin privileges to do that, get rights to to access financial data obviously or customer data or sales data or any of that.

11:11  
So I don't know how you want to do.

11:16  
You have multiple authentification, so in terms of multi factor authentification like obviously with any bank access that I do there's multi factor identification and I obviously I would do that online.

11:31  
So I'd be accessing AIB and there's lots of different annoying little things that I use to do that.

11:38  
And then obviously for the computer it's all like fingerprints to access it.

11:45  
So and then with Shopify there's different codes then with.

11:52  
Yeah.

11:52  
Like it's all it is all multi, multi device multi.

11:56  
Yeah.

11:57  
I suppose for OK for all.

11:58  
Yeah.

12:00  
But I didn't enable it.

12:01  
It's just more that it's on all those things already like OK, yeah, that might be good to imagine as well.

12:07  
I didn't press a button that say enable it, but I think, I think now everybody's apps and everyone's things, it's all defined by them as opposed to me.

12:18  
That's true.

12:20  
Yeah.

12:22  
So there's loads.

12:23  
Oh, I don't have a hardware token.

12:26  
There's SMSS and there's codes, Yeah.

12:28  
And then fingerprint.

12:36  
So again, you have to share some passwords sometimes to give someone access.

12:40  
And that's the way it works for, say, Facebook or Instagram.

12:44  
But what you can do is you can share.

12:47  
You add them as a staff or you add them as a collaborator.

12:51  
They they don't.

12:52  
I suppose they don't actually need a password, but you do share a link with them which allows them to access I suppose.

12:58  
Yeah, that isn't really.

12:59  
Yeah, no, not sure.

13:05  
The software enforces whatever passwords we need.

13:10  
So password managers like I sometimes use Google Manager passwords because but I don't actually for some of the I don't for the main business things.

13:22  
And the reason for that is I can access everything on the phone and the laptop and although Pixel and Mac they work OK together, just I I I prefer to have control to be able to change my passwords more regularly and to actually know them just if for any.

13:40  
Yeah, so password managers, but they're all saved and passed.

13:44  
So, like Google saves all your passwords in a password manager.

13:51  
Yeah.

13:51  
Is that like remembering your password when you go in?

13:55  
So I think the password managers were on about.

13:58  
We should be more specific there.

13:59  
It's like an actual separate application that saves all of your passwords.

14:06  
Then you obviously have a master password to get into that.

14:10  
That would be different.

14:13  
Well, I like the Pixel Fund does that for everything anyway.

14:20  
Again, I it's all fingerprint accessed, accessed, but it's not a separate app.

14:24  
Like I don't have a separate thing because it's like the most, I would assume.

14:30  
I think the Pixel security is pretty, pretty good.

14:35  
So, OK.

14:36  
Is that the right answer then, then?

14:37  
Yeah, yeah, I'd say I'll make notes.

14:42  
Blacklisting.

14:43  
No, I don't have to the force.

14:45  
Yeah, the software does that.

14:48  
So.

14:48  
So I'm trying to do training now.

14:50  
I suppose talking to you was ad hoc, no formal training.

15:02  
So like, I'm signed up to the different things.

15:05  
I've seen some videos, but I've never done a formal course.

15:09  
But like, I did work in Google for four years, so I did do a million security trainings there.

15:16  
Like, I think every month we were doing a new, new training.

15:21  
That's good.

15:21  
You have some experience all with it.

15:25  
Yeah.

15:26  
Yeah.

15:26  
Well, to be honest, quite a lot of experience.

15:28  
Like I was running a massive sales team there.

15:30  
So we, yeah, we had to do an awful lot of training.

15:35  
But yeah, it's different when you're, it's your own business obviously.

15:39  
OK.

15:39  
Are they reported?

15:44  
So again, this doesn't really work for like a business of my size.

15:47  
Maybe you're looking at slightly larger businesses like like I would obviously report something and so would any any like supplier that I work with would always inform me if they thought that the security wasn't strong enough on things.

16:02  
I think that's yeah, yeah.

16:05  
What do you think?

16:07  
Maybe somewhat would be applicable.

16:10  
Well enforced is a funny one, because I think consistently enforced suggests that there is someone with a role who is sending emails and that isn't the case.

16:18  
So is it consistently enforced?

16:20  
Yes.

16:21  
But it's as in no.

16:24  
I think #1.

16:25  
It's just there isn't just a person, an additional person who sends an e-mail to ask you to do stuff.

16:39  
I would be not sure straight away.

16:42  
I would probably call you.

16:45  
No, I've called my marketing team first of all.

16:50  
Also, I do have friends who have been hacked, so I'd probably call them as well.

16:56  
But yeah, there isn't.

16:57  
I wouldn't know exactly what to do.

17:02  
No I'm not a self treasure.

17:06  
OK for fine.

17:18  
Is this a tool or a survey?

17:19  
I felt this was more yes so it's meant to be a tool just for now.

17:26  
Like the This is the only kind of way we can use it, like use it at the moment.

17:32  
So it is more like a survey at the moment.

17:35  
But we're hoping then then when it's fully developed that we'll have our own website and this will be there, not in this format.

17:43  
Like it would be different and then that at the end it was feedback would spit out like tailored feedback specific to you.

17:53  
OK, so that's what our end goal is.

17:56  
But OK, this is where we're at now.

18:00  
Yeah.

18:00  
Because this felt more like, like, I suppose just a catalogue, a list of things that I'm doing or not doing.

18:12  
Yeah, Yeah, fine.

18:23  
You should probably, if someone's doing it, like, people won't be doing it with you, so they won't.

18:27  
No, no.

18:28  
Yeah, so you should always have If you're using any words that are like unusual, you should just always have an explanation for the what the terms are like.

18:37  
Add people do love the like other boxes.

18:44  
The problem with that, as you will be very aware is then your survey ends up with 50 million answers, which is OK for for reporting.

18:56  
Were they relevant?

18:57  
Yeah, so much beneficial.

19:02  
I don't know how beneficial it was.

19:03  
I'll be honest.

19:04  
I feel like I've just sort of, I I haven't learned anything.

19:08  
So and I don't know what to do next.

19:11  
Yeah, that's because we would hope that the feedback would be immediate, you know, when after someone's filled out and that's it would have like step by step instructions for someone so that, like, they're not just left, they're confused, like they know exactly what they need to do and need to do it.

19:32  
So we're working on that part now, but OK, great, great.

19:39  
Yeah, I think the intro like is, is more about you and less about me, OK.

19:57  
Just at a scam, I just sort of it's like I think it's quite obvious that you're not in the private sector.

20:04  
OK, makes sense.

20:06  
So it's it's like a research study as opposed to a customer facing tool.

20:16  
OK, That's good to know.

20:18  
So what I mean by that is.

20:21  
Like, I read a lot of research reports and it's they're just sort of more in turn, I don't know.

20:25  
I just get the sense that it's more about data gathering and less about business, business, problem solving.

20:32  
And so to say this was being done by a private sector company, I would nearly imagine you'd have at the beginning just a even a few sentences of like 75% of attacks are like happening.

20:45  
And like with with one hour a month you can actually solve some of these.

20:51  
The steps aren't huge in place like just sort of big picture setting.

20:57  
So there's there's none of that at the beginning.

20:58  
So imagine, imagine I I met you for the first time, which is sort of what's happened.

21:03  
There's no sense of this is this is what we're trying to do in the world.

21:10  
This is what we're trying to help you and protect you from.

21:14  
And the ask from businesses is just like an yeah, whatever.

21:19  
Whatever the proposition is, the proposition isn't clear.

21:22  
It's more like a research piece.

21:24  
Yeah, that's perfect.

21:26  
I'm just making note of that.

21:28  
Yeah.

21:34  
Like, would people be paying for this?

21:36  
No, it will be free.

21:38  
Yeah.

21:42  
OK.

21:45  
OK.

21:49  
I'd just probably make it more just customer friendly.

21:52  
Do you know what I mean?

21:53  
Like business customer friendly.

21:56  
Well, that's that's useful.

21:58  
Thank you.

22:05  
One question #50.

22:07  
OK.

22:24  
You see you're only sort of on phase, you're just you're using this to then fix this and then tailor it and then also look going through every forum, people just like to know how long it is.

22:36  
So, you know those sort of markers, yeah, because see there there is, there's two different forms and then there's different questions depending on how you answer it.

22:46  
So it's hard to to judge how long it will take, but it it has been taken between 5 and 1520 minutes for most people, I think.

22:56  
Yeah.

22:56  
But that would be good.

22:58  
I'll make sure to put that in as well.

23:00  
It's a progress bar like people like to see.

23:03  
Yes, that's good.

23:05  
Or how many questions.

23:06  
Yeah, OK, You you can't maybe do the exact number, but just a suggestion.

23:10  
Yeah, On it like, because it's great that people know what you're doing with the data.

23:15  
But again, that's why it feels quite like a research piece.

23:18  
Yeah.

23:19  
But maybe it is at the moment like that.

23:20  
It sort of is a research piece at the moment, isn't it?

23:22  
Yeah.

23:23  
At the moment it is like at the end, like, you know, you won't have to do the consent or read it all.

23:29  
It's.

23:29  
So yeah, Yeah, just boost it up a bit.

23:32  
Get some logos in there and yeah, I think that's that'll all come.

23:38  
But maybe when you're talking to people to say that or maybe you, you just want people to give you that feedback anyway, Do you?

23:43  
Yeah.

23:44  
No, the feedback is useful.

23:45  
Yeah, it is.

23:47  
That's perfect.

23:48  
Is that submitted and everything there, The perfect.

23:52  
I'll just come back here and I'll stop the recording.

23:59  
Stop.