**SME 5B RAT pilot call 23/04/2024**

Researcher’s voice in **bold**

**0:02  
Read the and see that question there.**

**0:06  
Do you consent to taking part in this study?**

**0:07  
And then it's got a list of questions.**

**0:09  
So if you can, if you can read those as you as you've clicked the boxes for me.**

0:14  
Yep.

0:15  
Do you consent to taking part?

0:16  
I do.

0:17  
I have read the information sheet entitled Information for Participants and I agree with it.

0:23  
I have had the opportunity to ask questions and as such understand the purpose.

0:29  
I understand I have the right to refuse to participate.

0:33  
I'm sorry, we've already talked about that.

0:35  
I understand that the answers I give will be collected by the research team and used in their study.

0:40  
I understand that the data will be used in the development of risk assessment tool.

0:44  
It is planned to publish in the findings.

0:47  
Just clarifying if you can hear me.

0:48  
OK and if I'm understandable.

**0:50  
Yeah, Perfect.**

**0:51  
Yeah, that's great.**

0:53  
Perfect.

0:54  
I consent voluntarily to be a participant in the study group.

0:57  
I do so moving on to the next risk assistant to are your sole trader.

1:03  
I am not organization.

1:05  
So how confident do you feel about the cybersecurity of your business?

1:09  
I would say about four or five, particularly because maybe I'm answering too much, maybe it's already going to come up, but particularly because we've already been through some negative things in the past and therefore we've beefed up our security accordingly.

1:24  
How many employees are there in the business?

1:27  
Equity, yourself and part time employees.

1:29  
There's currently 12 in the actual business.

1:33  
So it's smaller, but we operate in a length wider sense.

1:37  
What sector do you does your business operate in?

1:40  
Where we're education training mainly.

1:43  
So we're an aviation consultancy and training organization.

1:47  
I'm just looking for here.

1:50  
I would say education training is probably the one that's most relevant out of the list on there.

1:55  
So therefore correcting that, who's responsible for the cybersecurity of your business actually as a dedicated cybersecurity person team in house.

2:04  
So the way that we actually operate because we're a collaboration of organizations, we do have an internal team of 12, but we utilize the collaborations of others.

2:14  
So outside of them, we've got over 250 subject matter experts in small organizations that we work with are solely for training consultancy within aviation.

2:23  
One of those is an IT company and it's actually gone through their process of ISO 27,000 and one I believe it is for cybersecurity.

2:33  
I believe that's correct.

2:34  
And as such, we went through that process with them.

2:36  
And so they've incorporated, although we are not as approved, they have incorporated that into our quality management system.

2:43  
So it's a dedicated cybersecurity person is helping with that.

2:48  
Who are the dedicated persons responsible for IT and cybersecurity, IT cybersecurity only. Actually IT and cybersecurity because they also help with the development of our back, our back end as well and are integral within our content management system.

3:04  
Was the outsource persons responsibility for IP cybersecurity?

3:09  
Do they have cyber?

3:10  
Do you have cyber insurance?

3:12  
Actually we don't, but they do.

3:14  
And so we're kind of that's something we actually have to work on need to upgrade our insurance to include cybersecurity.

3:19  
So that's very good that that's been pointed out.

3:22  
So I do thank you for that.

3:24  
So I actually quickly know for them, can customers make purchases on your website?

3:28  
They can see now I need to as you go back and review double check that if our insurance covers, I know I need to make a quick note for our Chief Operating Officer.

3:39  
Sorry.

3:40  
Thank you.

3:56  
OK, I'm back to her after.

3:59  
That's why I like doing these things because you always need to double check.

4:02  
It's always good.

4:04  
Can customers make purchases on your website?

4:06  
Yes, they can.

4:08  
How do you take payments on your website?

4:09  
We process card payments directory.

4:11  
We use the party payment, all of the above.

4:14  
Actually we have combination of the first answers.

4:18  
Does your business currently comply with payment cards?

4:20  
That we do 100%.

4:22  
We made sure of that.

4:24  
Who are who has the ongoing responsibility of the same for security of your business website, outsource the party website has set up with a party specialist employee.

4:34  
So the same one technically is websites who sell with the party specialist.

4:38  
So the same one I mentioned before who's going for the ISO security, that's one.

4:42  
So they are integral part of it, but they are technically an outsourced third party.

4:47  
Do you feel confident managing the cyber security of him the business website?

4:52  
I do with their backing.

4:55  
I wouldn't if I was on my own without any other third party or without somebody who was integral.

5:01  
Who didn't have an understanding of the ISO accreditation of that.

5:08  
Is your website backed up?

5:08  
It is.

5:10  
Do you have inventory of our initial hardware used for your business, documentation of computers, mobile phones etcetera, blah, blah, blah?

5:18  
Yes, we maintain a comprehensive report somewhat.

5:20  
No, we do actually have that as part of everyone internal quality management system.

5:24  
We have that documented.

5:25  
Do you have an inventory of all the software they use for the business, again same as mentioned on their own content management system.

5:32  
So yes, we maintain that.

5:35  
Do you or your members of staff used to own personal devices?

5:39  
Some staff members do, but they're, but they are covered under our insurance, our actual company insurance as well for all of us.

5:47  
I need to double check about the cyber security aspect of that.

5:50  
But the, the, the backup of all the files and stuff is, is covered under that.

5:56  
Do your members of staff have full access to the business files when using their personal devices?

6:02  
They do.

6:05  
And again, that's making me question other aspects.

6:09  
Do you have antivirus and point management on your devices?

6:13  
Yes, all of them.

6:14  
And actually we've actually made sure that any of our employees who have personal devices that we've paid for antivirus and, and, and, and things on their personal devices as well.

6:25  
So we've covered that, but I'm not sure about the insurance aspect of it, although we have covered all our elements of it.

6:32  
Do you have spam or phishing filters enabled on your work e-mail?

6:37  
Yes, we do and and that's managed by the e-mail provider.

6:43  
So we use Microsoft 365.

6:45  
Generally, everything, are your work devices wiped off all data when they're no longer used for business.

6:53  
Do you know what?

6:54  
We've not actually came across that yet, to be perfectly honest.

6:57  
We are three years old and we've not actually had anybody leave that's had access to a work device.

7:04  
We've only had one person leave that only had access to an e-mail and they're personal and we've actually had that all wiped and we've run through the system that.

7:11  
So I would say yes for that because although it's not their own device, is part of the system like through e-mail and stuff.

7:19  
Is that correct?

7:20  
**Oh, yeah, yeah, yeah.**

7:24  
Is the data on the device backed up before wiping.

7:26  
Yes, because we actually backed up and reviewed everything before the individual left.

7:31  
And then we actually gave them a copy of what we did, how we did and make sure that we actually were made a copy, that we're no longer holding any other data as parenting to BR and everything.

7:43  
I wasn't personally involved in that.

7:44  
I'll be honest, it was our senior.

7:46  
But I do know that was taken care of according to legalities.

7:51  
How do you keep the software and devices up to date to manual update?

7:54  
We have automatic updates activated.

7:57  
We manually update some software and have automatic updates on other.

8:01  
We have automatic updates associated.

8:03  
We've manual update on some and have automatic on others.

8:11  
We haven't outsourced our party who puts this in for us noise.

8:15  
The third party, the the organization we we work with is integral part of it.

8:19  
The yeah, give us advice on that really.

8:23  
But we do ourselves, we manually update some in some of that are automatic.

8:27  
What type of data does your business collect?

8:30  
Personal data, emails, names?

8:32  
Yes, we do.

8:32  
Sensitive data, health related data, data, customs, recent ethnicity, yes, we do.

8:39  
Actually intellectual property, business sensitive, yes we do.

8:43  
We collect data, but I'm not sure what technology is of the above also, whereas I've got documents, receipts and that's intellectual property, but financial data as well would be an additional one.

8:57  
I don't know if that's that would be covered under intellectual property because we're done just sensitive data.

9:04  
**Yeah,** I suppose, Yeah, OK.

9:07  
Are you aware of the obligations in the GDPR?

9:09  
Yes.

9:11  
Are you, where do you store your data that you collect Cloud storage which got part and Microsoft 365 and also on another backup, so an an additional server as well.

9:25  
So that's on a work computer which I just put then on other backup server.

9:31  
**Yeah, perfect.**

9:32  
**Yeah, yeah.**

9:35  
**And so that's on site in the office.**

9:38  
It is on site.

9:39  
Yeah, yeah, yeah.

9:42  
**So you might just pop that in there as well with the OK.**

9:44  
Yeah, that'd be great.

9:51  
Do you encrypt the data that you store?

9:54  
I'll be honest, I don't know the answer to that.

9:57  
I'm assuming yes, but I need to double check with the third party.

10:01  
I need to double check that, So I'm going click.

10:08  
I'm not sure because that's the honest answer.

10:10  
Due process, customer payments over the phone.

10:13  
No, I've never done that actually.

10:17  
Do you share customer data with any third parties deliveries?

10:23  
Yes, because again, we're a collaborative environment and we have our own code of conduct within our quaility management system.

10:29  
So the ones that we actually designate as fellows out of the 250 odd companies and work with does me a bit like 8 fellows.

10:37  
So out of those ones that we do share all information with those.

10:41  
So yes, we have full access.

10:44  
How do you handle backup data backups for critical data?

10:47  
We have automated backups, We've performed manual backups.

10:50  
We have a combination of the first two.

10:51  
We have a combination of the first because we do some automatic and then the the manual ones to the servers that we know that on site ones that way.

11:02  
Is that right?

11:03  
How often do you complete a critical backup?

11:07  
I believe it's daily.

11:10  
I believe it's daily.

11:12  
I will double check, but I'm pretty sure it's daily.

11:17  
Do you have a, an immutable or air gapping gap gapped backups for your business critical data?

11:27  
I don't know to be honest.

11:29  
I need to double check that.

11:36  
**So it's the explanation given there of those is that that's is that clear to you or**

explanation is clear.

11:42  
Yes.

11:43  
And I have heard these terms, I've read these terms, but I'm not sure if we're actually doing that or not.

11:50  
I had a little bit of naivety on my part.

11:52  
I know that we do satisfy all points of ISO27001.

11:56  
I just don't know all of them.

11:57  
I just know that there's been a lot of people in the organization have done the actual quality assurance of those aspects.

12:03  
So I'm assuming that we would have if it's a requirement, if it's not a requirement, I'm not sure.

12:08  
I'm not sure if this is actually a requirement or not on that because I've read it.

12:12  
I've not seen it on any of the critical checklists.

12:17  
I'm not sure, but that might be me that that's missed it.

12:21  
So I'm I'm just written down.

12:22  
I'm not sure at this point.

12:25  
Are you your data backups tested again?

12:31  
I'll need to double check how often they're they're tested.

12:34  
I know they are tested.

12:35  
I don't know how often top and I'm not sure because I I know they are tested, but I'm not sure how often they're tested.

12:47  
Do you enforce access control so that different users have different access right?

12:51  
Yes, we do.

12:52  
Do you have multi factor authorization?

12:56  
Yes, we do on everything actually for for business and critical applications where possible.

13:01  
Yes, for some.

13:02  
So yes, for for all business and critical applications where possible.

13:06  
We do have what type of multifactor of MFA do you have?

13:11  
Click on that by authorization authenticator app.

13:17  
We don't have hardware tokens.

13:19  
We have e-mail codes and SMS codes as well depending on system.

13:23  
That's one of them 3 usually.

13:26  
Do you have any other?

13:28  
Do you or any employees share passwords with one another?

13:32  
No, no we don't.

13:35  
The only time I'm thinking no, I don't on there, but the only time the passwords are shared is if there is ever a problem where it has to be a full reset, it's directly from one of the board members to that employee and then share the password's not shared, but the time instance and when it was done is shared.

13:54  
So there's always a backup of it knows when that employee got a new password for example and that information is kept within the board.

14:02  
But whoever is actually responsible for at that time moving on the backup and generally we don't actually see it either.

14:08  
It's actually generally because I know I've done a few times and it's like been forwarded to them and then they get told to reset right away as well.

14:17  
So in theory, no, we don't share any passwords.

14:20  
**Yeah.**

14:22  
Do you require staff's passwords to have a, a minimum length?

14:27  
Yes.

14:28  
Again, keeping with the, you know, the same as Microsoft 36, I think I keep with that standard route.

14:34  
It's got to have uppercase, lowercase, numbers, letters, other elements to it, so on and so forth.

14:40  
Do you advise staff to use a password manager?

14:43  
No, I don't actually.

14:46  
It stores all of the passwords.

14:48  
I don't advise it.

14:51  
I don't enforce either.

14:52  
I don't advise it and I don't.

14:54  
So no.

14:56  
Do you enforce block listing passwords?

14:59  
Where this is where certain passwords are not allowed as they are too easy to guess.

15:05  
Yes, they're not allowed.

15:06  
Anything that's got the business name in it, for example, or like 2024 or whatever it might be.

15:12  
So yes, the business configurations this, yes, the software forces this.

15:17  
So yes, as a business, we configure this.

15:19  
We make me tell them that it's not generally the software that does it says how often do you and your employees engage with cybersecurity training?

15:31  
Because we're at the start of this we've not actually trained all employees on everything yet.

15:36  
I've not actually read the answers.

15:37  
Yes, staff are required to engage in Cyber Security training months and months.

15:41  
Yeah, once a year staff are informed the precise security on a ad-hoc basis.

15:44  
At the at the moment is that we will be upgrading that in the future.

15:48  
As of June when we're fully complying with everything and we know the we're going to be all everything we've all be doing monthly minimum updates and training on all staff.

15:59  
But at the moment it's at all.

16:02  
What methods of cyber security training have your your staff undertaken?

16:07  
Combination of all actually.

16:13  
Videos, presentations, you know, community announcements, courses.

16:16  
Yeah, combinational law, our employees required to report any suspicious activities.

16:21  
Yes, they have.

16:23  
Yeah, they, they do they, they're required to yes, we have a clear reporting procedure.

16:26  
We do actually have a clear procedure for it.

16:29  
Someone if not, we have actually have a clear procedure for reporting and we actually have a dedicated e-mail address to all employees there's specifically for this as well.

16:40  
So they're all recorded separately and then we report back on, whereas to Microsoft, whatever else as well.

16:47  
Would you or your staff know what to do if a cyber incident occurred?

16:53  
Yes, to the certain degree at the moment of if they know that they occurred, they basically tell one of the board members, and we've got that third party who's always there, who's part of the business.

17:03  
It's a strange same third party because they're a fellow of their organization.

17:07  
So we always refer to them.

17:08  
So yes, there's a plan in place, a little bit ad hoc at the moment, but the plan.

17:13  
But there is actually a process in place to be reviewed.

17:16  
But there is a process in place.

17:18  
Yes, I have a plan in place, but only some staff are aware.

17:20  
No everybody's aware of it.

17:22  
It's just it has to be refined and that's the thing that I know has to be refined.

17:27  
But we do have a plan in place and that all the staff are aware.

17:31  
Have you tested your incident report plan?

17:34  
We've done minor testing on it, to be honest.

17:36  
So yes, it's tested regularly and updated.

17:38  
Yes, once.

17:40  
I would say yes, once because it's not been done regularly and we've done a few times, but we've not done enough to say that it's in place.

17:49  
Do you have a business continuity plan?

17:54  
Yes, it's regularly tested.

17:56  
Yes, but it has only been tested once.

17:58  
Yes, but it has never been tested.

18:00  
Yes, but it's only been tested once.

18:02  
As the honest answer to that, please follow link to if you are an employee's business, don't you don't tell me, OK, so I'll pass that on to an employee then or you want me to do that as well.

18:22  
So publish that question there Crystal with a link.

18:25  
If you are the only employee in your business.

18:27  
I know I'm not the only one, but can I like to pass it on to other people in my business if that's OK?

18:32  
Oh, yeah.

18:32  
No, that that's, that's not allowed.

18:35  
Is that?

18:35  
**No, no, it's, it's at it's actually not to do that at all.**

18:38  
**It's like, do you know the first question was, are you if you're a sole trader?**

18:42  
**So that's actually for that.**

18:43  
**So if you go back to the, the page where you were answering the questions, there should be another link to say submit.**

**18:49  
So if you could follow that one.**

18:50  
Yeah, it's just next.

18:51  
Yeah, yeah, yeah, yeah, yeah, yeah.

18:53  
**And then there should be a little survey there for you to complete by the feedback.**

18:57  
Yeah.

18:57  
Thank you for waiting.

18:58  
And we start the feedback.

19:02  
No, it was understandable.

19:03  
Was the language understandable?

19:05  
Was very understandable.

19:06  
Was not jargon used?

19:10  
Yeah, I suppose if somebody's not gone through anything, like I'm still at the early stages of it, so I'm understanding parts of it.

19:17  
But I suppose that some of the jargon used would not have been understandable if you've never heard it before.

19:24  
Does that make sense?

19:25  
Yeah, Like air gapping or stuff like that.

19:27  
And I, I, I would say that some of the kind of maybe older generation ones that aren't involved at all, that would be non language that they wouldn't understand.

19:38  
**Yeah, yeah.**

19:40  
So I'm putting down the four-star for that because I think, but I think that's something that maybe needs to be reworded for those who are the very, very earliest stages or don't have anything at all.

19:49  
Yeah, please comment on the language used.

19:52  
I actually just said that, so I'll just put that as a comment there as well.

19:57  
**Yeah, I think it's you'll have to put something into the boxes to so the thing will submit anyway.**

20:03  
So OK, still was easy to use.

20:25  
Yes, still was easy to use.

20:27  
Please comment on use as well.

20:28  
Just so I'm just writing easy to use on my organized.

20:41  
Great.

20:45  
If I can actually spell organized, that'd be good.

20:48  
My questions are relevant to my business.

20:50  
They are very relevant.

20:52  
I'll pick a five out of that because I'm actually making the comment on the relevance that it made me question additional items and as such it was very relevant.

21:13  
Was it beneficial exercise again, yes, same as above.

21:17  
Some works pretty copy and pasted the same answer because it's that's why.

21:21  
Do you have any other feedback?

21:26  
I don't have any other feedback other than I'd like to continue to be involved with these types of initiatives as they bring awareness and it's something I'll be sharing with the team and I think it's very beneficial that.

21:39  
That's great.

21:40  
**No, that's good to know because we're kind of developing it kind of iteratively.**

21:45  
**So we're going doing a few workshops with people in the upcoming weeks.**

21:50  
**And once we get that done, we're hoping to launch a website and we're hoping to test that website so we could be back to to have a look at the website.**

21:59  
**And as we go on, there'll be more information that's useful for you.**

22:02  
**Do you know if we're kind of just building up the information as we go?**

22:05  
I appreciate that.

22:06  
**Yeah.**

22:06  
**Each time you engage with us, hopefully there'll be kind of more more stuff to be learned.**

22:11  
No, it's really good.

22:12  
It's really fantastic, really promising.

22:14  
Thank you very much for it.

22:15  
Thanks for letting me be involved with it.

22:17  
It's always better for my organization.

22:20  
Hopefully it gets better for others as well.

22:22  
**That's great.**