

# The Digital Access Show

## Season 3 Episode 14: [Luke] Irwin

### Introduction

[music playing]

[Narelle]

Hello, and welcome to The Digital Access Show. Take two for this particular episode. Yeah, you know, when you have a severe vision impairment, you sometimes forget to do one thing, press record.

So, my guest, Luke Irwin, has been very, very kind. Let me know if he's laughing, because obviously, I don't know. He is from Aegis Cybersecurity.

And Luke has been on before, minus the one where I forgot to press record. But Luke's been on before to talk about the vulnerabilities that people with disability do have over and above a normal person.

Luke, thank you so much for coming back.

[Luke]

Not a problem. Happy to be here and happy to help.

[Narelle]

And we have doubly confirmed that we pressed record. So, let's get into it. [Luke], tell us a bit about yourself.

### About Luke and Aegis Cybersecurity

[Luke]

So, I am Luke Irwin. I run a cybersecurity consultancy called Aegis Cybersecurity, based here out of Brisbane that's servicing Australia.

I specialise in governance, risk and compliance, and fractional chief information security officer functions. That's looking at what the business needs, how to do it, and ensuring the organisation has the culture it needs to achieve it.

The point of difference that Aegis has when compared to other cybersecurity consulting firms is that we don't sell hardware, software, or managed services to deliver our recommendations.

That removes the conflict of interest from our advice. If we say this is what you need to do, it's a statement of fact, not a sales pitch.

### **Digital Dependence and Risk**

[Narelle]

One of the things people forget is that people with disability probably use digital tools just as much, if not more, than others. That's a big vulnerability for us, isn't it?

[Luke]

Oh, it's massive. The level of scams targeting people without disability is already high.

If someone has a vision impairment, their ability to pick up visual cues is reduced, which increases the likelihood they'll be taken advantage of.

### **Real Life Example: The Tinder Incident**

[Narelle]

I've got a Tinder story to tell you. Somehow one of my email addresses got linked to Tinder. I am definitely not a Tinder person.

Trying to unsubscribe was a nightmare. They said click unsubscribe, but I'm not even on the app. And I'm blind, so I'm not downloading an app just to unsubscribe.

[Luke]

That's what we call a dark pattern. It's designed to make it harder to opt out.

Even for someone fully sighted, it's frustrating. Add vision impairment and it becomes another barrier.

### **Data Breaches and Growing Threats**

[Narelle]

Scams are everywhere. We've had breaches from major companies. How can a normal person protect themselves, let alone someone with disability?

[Luke]

These breaches create rich data sets. Hackers can build a detailed picture of a person and impersonate them.

For someone with a disability, managing the fallout is even harder. You may need to review documents or systems that are not accessible.

### **Cognitive Load and Fatigue**

[Narelle]

There's also disability fatigue. That cognitive overload makes mistakes more likely.

[Luke]

Exactly. Cybersecurity relies on people being right every time.

That's unrealistic. The added cognitive load increases risk, especially when combined with daily challenges of living with a disability.

### **Accessibility of Security Tools**

[Narelle]

What about tools like antivirus or security apps? Are they accessible?

[Luke]

I doubt they are fully accessible.

But there are some helpful tools. Multi-factor authentication can improve security, though it adds complexity.

Password managers are also useful. They reduce the need to remember complex passwords and can improve both accessibility and security.

### **Banking and Everyday Barriers**

[Narelle]

Banking is a big issue. ATMs, EFTPOS machines, PIN numbers. I've had to tell people my PIN just to pay.

[Luke]

These systems are built for the majority, not for inclusion.

Chatbots are another example. They may not work with screen readers or allow voice input, which creates barriers.

### **CAPTCHA and Verification Challenges**

[Narelle]

Those puzzle verifications are terrible. The distorted audio is really hard to understand.

[Luke]

They're designed to stop bots, but they also exclude people with disabilities.

It's a trade-off between security and accessibility, and right now it often leaves people behind.

### **Who Is Responsible?**

[Narelle]

So who is responsible?

[Luke]

Organisations have an ethical obligation to make products accessible.

But many focus on the majority and ignore the rest. It's a cost decision, not an inclusive one.

### **The Business Case for Accessibility**

[Narelle]

They forget that everyone ages and experiences changes.

[Luke]

Exactly. By ignoring accessibility, they reduce their potential market.

It's not just one percent. It includes older people, people with language barriers, and more.

### **Practical Tips for Businesses**

[Luke]

Businesses should design with accessibility from the start.

Use clear layouts, avoid reliance on mouse-only navigation, and include features like alt text.

Engage accessibility experts early. It's cheaper and more effective.

### **Practical Tips for Individuals**

[Luke]

For individuals, question what data is being collected.

Ask why it's needed, how it will be stored, and when it will be deleted.

Only provide what is necessary.

### **Data Collection Concerns**

[Narelle]

I've never thought to ask those questions.

[Luke]

Most people don't. Organisations often collect more data than needed.

Minimising your data exposure reduces your risk.

### **Hidden Accessibility Gaps**

[Narelle]

Here's another issue. Passport numbers are not readable for many people with vision or cognitive challenges.

[Luke]

That's a serious gap. It forces reliance on others, which creates new risks.

Your passport is a key identity document, so that dependency is a concern.

### **Closing Thoughts**

[Narelle]

We've gone down a few rabbit holes again. [Luke], how can people contact you?

[Luke]

You can reach me at [lirwin@aegiscyber.com.au](mailto:lirwin@aegiscyber.com.au) or find me on LinkedIn. Happy to help and point people in the right direction.

[Narelle]

Luke really knows his stuff.

Please go and have a chat with him and keep yourself safe online.

Think about how many email addresses you have and whether you really need them.

Please like, share, and subscribe to The Digital Access Show. We really appreciate your support.

[Luke]

Congratulations on your growth.

[Narelle]

Thank you. Have a great week, everyone, and we'll see you next time.

[music playing]