**Jacob Bellas** (00:05):

Hello. I'm Jacob from Contractor Voice. I founded Contractor Voice to champion contractors working in the temporary workforce space. I experienced first-hand the malpractices undertaken by parties in the supply chain, and I'm acutely aware that they continue, and that contractors are falling victim to multiple forms of abuse still today.

This podcast will focus on the recent and unfortunate cyber-attacks, targeted on umbrella accredited through the organization well known to us as the FCSA, the significant consequences to contractors, and how they should be protected against cyber-crime perpetrated on their employers.

**Jacob Bellas** (00:36):

My two guests today are well known in the sector for being very vocal about the rights of contractors, and bringing about change in the industry to protect them. I'm joined today by Umbrella owners, Rob Sharp of Orca Pay Group, and Drey Francis of Compass Contracting.

Welcome to the both of you. So, gentlemen, what are your opinions on the recent FCSA umbrella cyber-attacks, and the impact upon contractors?

**Drey Francis** (00:56):

Well, thanks for having us on, Jacob. Obviously, Rob and I saw the recent LinkedIn posts that you put out there, and knowing the industry the way we do, we wanted to reach out and take part in this. So, we appreciate you having us on today.

I think main concerns for me personally is, I think a lot of people are focusing on the cyber-attack towards the umbrella company, not a lot of people are focusing on the actual person who's felt this the most, which is the contractor. The fact that their personal data is now out there somewhere, because businesses weren't able to control their cyber security.

I think that, for me, is the main thing that people really do need to focus on. I think as umbrella owners, we probably have a duty, not probably, we definitely do have a duty to protect our contractors and the data.

**Robert Sharp** (01:49):

I echo that. I think it couldn't be a worse scenario for those affected. I think what scares me is at this stage is, has any data been compromised? I think that would be the first question, that if I was an employee, if that happened to us I know that the first question my employees would ask us is, has our data been compromised?

Cyber-attacks can happen in any walk of life. We've seen Sony, Easy Jet, BP. I think Sainsburys, was it Nectar? Unfortunately, it's part and parcel of the reality and the world that we live in these days. I think the last thing I read stipulated that cyber-crime now contributes to the highest levels of income for criminals. That alone tells you just how prominent it now is.

**Robert Sharp** (02:47):

I think it's also important to have a bit of empathy here for the businesses that this has happened to.

I'm with Drey. I think that the largest empathy and thoughts go to the actual individuals. Our job, as umbrella employers, is we are responsible for paying people their livelihoods, and one can't detract from the fact that this has caused a very, very big problem for those contractors that are employed by those umbrella companies unfortunate enough to have been victims of this. So, we can't overlook that.

I think that for me, is really where I fear the most is, is there anything as a consequence of this that will actually now put that information of the employees out there, in whatever realms of the internet or online or however that it can be. So, that would probably be the biggest question I'd want to ask.

**Jacob Bellas** (03:45):

Yeah. I think there's a very good point that you raised there actually, it's the contractors that have been overlooked a lot of the time here. So, do we know which companies have definitely been affected by these recent attacks?

**Robert Sharp** (03:55):

My understanding is that it is both Parasol, I think a couple of their sister companies, SJD and Nixon have been affected, and Brooksons. Drey, correct me if I may be incorrect there.

**Drey Francis** (04:09):

Yeah. Yeah. I mean, it appears there's a group of companies that have been targeted. There looks like they all have one thing in common, not just being umbrella companies, they are all members of an organisation. The problem is it seems to be the biggest ones that are highlighting this, but there are 600 umbrella companies in the industry, so you can't account for everyone who's been attacked.

**Jacob Bellas** (04:33):

So, why do you think the payroll industry's been targeted by cyber criminals?

**Robert Sharp** (04:39):

Honestly, I don't believe that it is the payroll industry as a whole. I'm sorry, I'm not going to win many friends for this, but I think that this is a continuation of a same attack that started in the summer of last year and is directed against one organization in particular.

We've had fake Twitter handles, we've had confessions from CEOs, or false confessions should I say, from CEOs. We've had cloning of the organisation’s website; we've then had cloning of their umbrella members.

Now, I'm sorry, but I don't believe it a coincidence that the three founding partners of the said organisation have actually been a victim of these cyber-attacks. So, look. This for me is where it becomes dangerous. I understand that people have to control narratives, but this is where the industry as a whole, I basically feel now that this has had a detrimental effect on the industry, because it's been deemed an industry problem. Which is now, for want of a better terminology, probably put an advert out there for real cyber criminals to actually target and look at our industry as a whole.

**Robert Sharp** (05:54):

I've read articles about this being as a result of the increase in contractors who have fallen inside IR35 and then obviously being put through umbrella companies. Umbrella companies have existed for 20 plus years. The big ones are always cash rich.

We had the off-payroll reform in the public sector, and never before has there been anything like this. So, I think we need to be very, very careful on who and how that narrative is being controlled. I think that it sets a dangerous precedent to do that, and to actually... Drey and I know this better than anyone. Unfortunately, when one is tarnished, we're all tarnished. We have 600,000 plus contractors who are using a variety of umbrella companies, who now, probably rightly, are sitting there wondering who's going to be next, and if they'll be next.

**Robert Sharp** (06:50):

So, I'm sorry, but I feel like I have a responsibility, in my very humble opinion, I don't believe this is an industry specific problem. I believe it now can be, but I believe that this has been a sustained attack on an organisation, and it is a continuation from, like I said, from what has commenced in the summer.

**Drey Francis** (07:13):

To add to that, I think if you look at the umbrella industry, it's grown in popularity through legislation, not necessarily the popularity because people automatically choose umbrella companies. But with government legislation over the last four years, a lot of people have been forced into umbrella companies, and as such the valuation of that industry has gone up.

So, you look at some of the biggest players in the market, and they're probably a billion turnover, to cyber criminals that's quite a hefty target. While agreeing with everything Rob's saying, that it does need to be focused on a core group of individuals, who've maybe touted themselves as the biggest and the best, I think potentially that is why they've been targeted. But I think the industry itself has actually grown in size and turnover, so in essence that has led us to be targeted by these people.

But to revert to Rob's point, there is a very small percentage of this industry that has been targeted, so I don't think it's entire industry that's at risk.

**Jacob Bellas** (08:16):

Yeah. So, you pick up there on some of the largest players in the industry, and the FCSA for example, is a massive player that deals with some of those largest umbrella companies. But

I saw on their recent article, I think it was posted middle of January, that that organisation doesn't have any control on how its members deal with IT security, to avoid these cyber-attacks.

I think I'm right in saying that a couple of the umbrella companies that have suffered recent attacks hold membership, and I think that, particularly in light of the fact that we're talking about the contractors that are at risk here, whether their data's at risk, whether they're being paid or not. It would be up to the organisation that's governing large numbers of umbrella companies to introduce measures going forward, that's going to assist in preventing attacks like this, and setting standards in the industry that's going to ensure that this isn't happening, or that companies are prepared the most they can be, to do so.

**Jacob Bellas** (09:19):

I know that the all-party parliamentary group has shown an interest in this as well, knowing that these recent attacks are ongoing, and trying to dig to the bottom of some answers and how the industry can move forward with that.

So, if it is only certain areas of this industry that are being targeted, what are, and I pose this to either one of you, what are your recommendations that can be done proactively to protect contractors going forward?

**Drey Francis** (09:48):

For me, I think my first word of warning to this entire industry, whether you've been a victim of these attacks or not, is to grow up. I think, we place far too much emphasis on an accreditation. I'm an accredited business, that makes me safe and secure. Well, I think we need to start reevaluating what that terminology actually means, because just because someone checks that you're doing everything correct on a payslip, doesn't mean you're taking your responsibilities as an employer seriously enough.

If anything, this has highlighted that as an industry potentially we need to look... Well, actually, no, not even that. As certain accredited bodies who claim to be the biggest and the brightest and the best, I don't think they've gone far enough in their claims to being industry gold standards, because this is just a glaring example of maybe people are looking at the surface of things and saying, right, tick box exercises completed. But what have you done to put yourself in the position that you are claiming to be the biggest, the best, the brightest?

**Drey Francis** (10:51):

So, I would say to those businesses, to anyone in this industry, I think it's time to grow up and start looking at our responsibilities. We account for hundreds of thousands of people employed by umbrella companies, as Rob said, and it's time to be a proper grown up business, and be responsible for those people who trust you to be their employer, who trust you to handle their payroll. They also trust us to handle their data. So, the first thing I would say is to those accredited bodies, do more, like protecting employees data.

**Jacob Bellas** (11:20):

Yeah. I think you'll have seen my letters to the regulators recently, where I was making recommendations to them to actually not look at accreditations, but instead to look at the practices that the companies have, and the protections that they have in order, for the benefit of the contractors. So, rather them looking at mandating certain accreditations into PSLs, they should actually be looking at what a company's ISO regulation standard is. I made recommendations for the ISO, 27,001, and I think- Yeah. Go on.

**Robert Sharp** (11:53):

Jacob, I think, you've mentioned the all-party parliamentary group there. It'd be remiss to sit here and not actually reference the government as a whole. We're talking, and this is going to seem a little bit like I'm digressing and going off topic, but actually I'm not. We have, as an industry, been left unregulated for... Well, ever since the inception of umbrella companies really. Now, when you leave an industry that deals with billions and billions and billions of pounds of livelihoods by the way, which is what this is, all the monies that go through our businesses are the livelihoods of our employees.

If you look at the FCA, the Financial Conduct Authority, anyone who is FCA regulated, as you quite rightly pointed out in the letter, and I did actually read that on your post, and a lot of the content in that was spot on. You're asking for what is, and should be, a minimum standard to protect the critical information of your employees.

**Robert Sharp** (13:00):

Now, it's easy to jump on the bandwagon and I will say this. I agree with Drey very much so, about for years and years now we have got this mythical mindset that an accreditation makes us bullet proof. The simple truth is, as we are now seeing, it doesn't. It affects the whole supply chain when individuals, employees of those umbrella companies, are not being paid. It has a knock on effect on the umbrella company that has been the victim of this. It has a knock on effect to the agency who has found the work for the individual. That has a knock on effect in the end to the end client, where that individual is actually conducting his or her skillset. So, the ripple effect is substantial.

Look, Drey's nailed it on the head here. The simple reality is that it's the responsibility of each business. So, I have a responsibility as Orca Pay Group, to make sure that our cyber security is robust enough that this can't happen. Drey has a responsibility for Compass to ensure that that can't happen.

**Drey Francis** (14:13):

For anyone who's been involved in our industry for a long time, and this might be a very contentious thing I'm going to say, but it has been self-regulated. If we want to talk about this FCSA accreditation body here, it was founded by members of the industry. So, it's not like a government body that's come in and regulated us and said to us, "By the way. As an industry, you need to have your cyber credentials at this point."

Jacob, you mentioned the ISO accreditation there. I think everyone should be working towards those. But what has happened is we've self-policed ourselves, and it was always easy to just take the easy road, because all you had to do was complete the tick box exercise.

**Drey Francis** (14:51):

I know I'll get a lot of hate for saying that because people talk to me about the audit being stringent, and that's fine. But the fact of the matter is, it has been a self-policed industry to this point. What Rob is saying, what I'm saying is, it's time for the actual policing to start. It's time for people to come in and say, right, forget the fact that you've said and done the things you're going to do to earn accreditation, prove to us you have done the things you need to do to protect your contractors' data.

**Jacob Bellas** (15:17):

Yeah. My letter did get a response from BEIS who said that, unfortunately, areas that I was requesting that they promote change, were out of their remit for regulation, and therefore they couldn't advise. However, I do think that as they have a responsibility in regulating employment businesses, there is more proactive measures that they can take in preventing incidences like this.

**Robert Sharp** (15:47):

I think that's a sellout, Jacob. I think their response to you is a sellout, and is an absolute, absolute dismissal of what they know to be their responsibilities. I'm absolutely gob smacked. But unfortunately unsurprised that that's been their response. I really am. Do you know what? It just sums up our point about the fact that they have left an industry that is responsible for that much money to police itself.

Then they wonder why... Let's have it right here. The last two years have been the worst reputationally for umbrella companies that I've known of in 17 years in being in this industry. You're talking about a select few, who are causing the effect of everyone else to be tarnished with that same brush.

There are so many good umbrella companies out there, who have got their security, their cyber security, as good as they can have it, who know that their responsibilities are, and what their responsibilities are for their umbrella employees, that I think that is so short-sighted from BEIS.

**Robert Sharp** (17:06):

Now, let's have it right, as well. They've put the single enforcement body, that is a BEIS announcement. So, what I don't understand is they announce that, and they've announced what the plan is, and that single enforcement body will have the responsibility of regulating umbrella companies. So, that's their announcement. So, their response to you, of it's not in their remit and it's not their responsibility... People's details are online. People's identities are now able to be stolen, and that's not their responsibility?

Don't just leave it to us. I'm not arrogant enough to think that I'm going to change the world, and neither is Drey, but you know what? We're trying to fight the fight. Give us something government.

**Robert Sharp** (18:01):

You know full well what is going on. The industry knows full well what's going on. Fed up of seeing posts on LinkedIn of everyone saying, "Oh, we shouldn't be jumping on the bandwagon because these people are suffering, and these businesses are suffering." You've caused it. Do you think if McDonald's, it got found out that McDonald's hamburgers were made with horse meat, that there wouldn't be an issue from that? Do we honestly think that? Do we not think that the world and governments would not ask questions about that?

Yet we've got an industry that is being hacked left, right and center, that is responsible for billions and billions of pounds a year and people's livelihoods, and actually, "Well, that's not our responsibility." These people, the nurses, the teachers, the social workers, the people in COVID for the last two years, that made sure we are all okay, are now the victims of this, and it's not their responsibility.

**Jacob Bellas** (19:06):

Well, thank you very much, gentlemen, for taking part and taking time out of your busy schedules. Thank you for talking about your experiences in the industry, what's going on at the minute, and any recommendations.

Do either of you have any final words or anything else you'd like to add?

**Drey Francis** (19:22):

I mean, if I can just say, again, from my side, I'm sure from Robs, we appreciate you having us on to discuss matters of this importance. I think there's not enough being done from the protectionisms of the contractor. Knowing that someone like yourself is out there airing these really, really important views that people can actually listen to them, understand what's at risk, have someone that they can come to, and to touch on a lot of the points that Rob has touched on within this.

I would just say, people need to speak up. If you're worried about the company you're working with, or you're worried about how your data's been handled, there are places to go.

**Drey Francis** (20:08):

Speaking to people like yourself, Jacob, where contractors, they shouldn't feel like they've just got to be a commodity in this industry. They should realise that there are places they can go, to raise these concerns.

All government may not be stepping in to protect a lot of the contractors, you do have people like yourself. I mean, Rob's one of the best operators in the industry. If you ask anyone about someone who's passionate and cares about doing the right thing, reaching out to Rob, people like myself, we're all here to help raise awareness of these really, really important matters.

**Robert Sharp** (20:40):

I just echo everything Drey says there. But there's a lot of smart, good people in our industry, and I think sometimes as an industry, we don't collaborate enough. We've got smart minds, but it's very dissected, it's very individual. You are this accreditation or you are that accreditation or you're no accreditation. Something isn't working anymore, and is it not time to sit down and think, well, can we change tack? What can we do? What can we collaborate on together, that really does show that we have the best interests of our umbrella employees at heart? I don't mean just mine as Orca Pay Group, or Drey's Compass, actually the industries as a collective. I think if we sat down and actually came together, I think we could do a lot of good. So, I'd champion that all day long. But aside of that, I whole heartedly agree with what Drey said there, without any hesitation.

**Jacob Bellas** (21:51):

Fantastic. Well, thank you to the both of you, and I hope you'll join me very soon.

**Drey Francis** (21:57):

Thanks. Appreciate that.

**Robert Sharp** (21:58):

Appreciate that.