Dave Tait

There's a stat, I think over 80% of British businesses have been subject to a breach and that was 2020/21 and that's stats that have come from the National fraud intelligence bureaus made from these action fraud reports, and they think that's massively underreported.

Ajay Bains

Welcome to the Demystifying Cyber Podcast by Lancashire Cyber Foundry. I'm your host, Ajay Bains. I currently work as a Business Support Officer for the Lancashire Cyber Foundry. We're passionate about helping businesses to realise their digital potential. We work with eligible organisations across Lancashire to support them with placing cyber innovation at the heart of their strategy. Today we welcome a special guest, Dave Tait. Welcome, Dave.

DT

Thanks for having me here, Ajay.

AB

No problem. Dave is currently a Detective Sergeant for Lancashire Constabulary Cyber Crime unit. Thanks for agreeing to be part of our podcast series. It's great to get numerous perspectives on the cyber landscape as this offers diversity of thought and as the current Detective Sergeant for Lancashire Constabulary Cyber Crime Unit. I'm sure you can offer some unique and valuable insights into the world of cyber. So, to begin with, I want to delve into your background to date and what led you to your current role as Detective Sergeant for Lancashire Constabulary Cyber Crime Unit.

DT

So not taken what many might say is a traditional route. I've not come from a computing educational background or not any skills per say in the cyber world, anything formal. In the past it wasn't something I was looking to do. Coming from a law enforcement side, though, I've been a police officer for 17 years. The first 10 years of that, I was a uniformed frontline officer dealing with your day-to-day general crime victims, that kind of stuff. And I did- I really love doing that- I had done for about 10 years and I got to the point where I felt like I was ready for a new challenge. So in the police and I feel how it works, but you can become a become a detective. We call it a trainee investigator. You go for a accreditation process to become a Detective Constable and you'll be dealing with more serious, complex crime. Running your own investigations and I thought that's something that I'm interested in. So yeah, started doing that. And I loved that. I became a DC, I worked in lots of different departments. As a general CID department dealing with serious crime works in child protection. And I've worked on some quite major investigations, so quite a wide range of stuff, and this is where the cyber the digital side comes in, because what I started to realise was that every job we dealt with, every incident I investigated had some form of digital element to it. Whether that's the suspect, the offender, using cyber, using the Internet. Using digital devices to commit the offence and to giving that wider reach, so to speak, and bigger impact. Or whether it was digital investigation strategies coming in and using digital forensics digital stuff to follow lines of inquiry and ultimately lead to a prosecution. There was both sides that were coming more and more, and I like that side of it I like the methodical, the online stuff and we use a lot of Internet of Things, mobile phones, that kind of stuff. So, I kind of set my stall out as Detective for that to be my area of, shall we say, expertise that wanted to go down, went on training courses, continues professional development days, anything to do with digital I would jump on and upskill myself, really. And that's gave me a bit of a new lease of life in policing and I enjoyed that side of it. So, then the next step when the opportunity came up to move into our cybercrime unit was the right thing to do. I'm not going to lie, I was a bit apprehensive because not coming from that technological background, digital is one thing, but when someone mentioned Cyber, you think that's like that's beyond me, you know you have that hacker image that everyone has straight away. I thought I'm going to walk into an office, duck out of water, so to speak, it wasn't quite like that. But anyway, I went in and realised that, yeah, this is for me, this is what I like doing. So, I was there, what we call a pursue investigator. So, like a detective in the Cyber Crime Office dealing with Computer Misuse type offences, really enjoyed that. And then obviously that moved on and the options came up to get promoted within that department and applied to be the Sergeant and yeah we’re sat here now, so that's kind of my journey in cyber. It's not come from technical. It's just from the law enforcement side and the investigation side of.

AB

Yeah. Perfect. Thank you for that. And I was going to kind of delve into to cybercrime, but just wanted to ask off the back of that. Do you think that the kind of transferable skills that you're taking from your previous roles in policing have supplemented your current role now? Have you been able to harness them in this role?

DT

Oh yeah, massively and it's something I think as police officers were guilty of quite a lot not realising the skills that you have, generally doing that job, I mean communication, speaking to members of the public, the resilience, the- you have creative thinking sometimes to solve a problem- all these you kind of take for granted. And it's not until you are maybe out your comfort zone. Like I said I was, that you start using these skills and a lot of my job is talking to people who may not be cyber aware or technologically minded and bringing this world to them and saying this is what you need to do. This is- this is where you need to be. I don't want to use the word dominate down, but yeah, using the appropriate language for your audience. So yeah, those skills have helped massively, and I was a bit apprehensive about moving into cyber. I thought it was a bit too much for me. They said “Well, it's like a cyber investigation as a police officer, like any other investigation. But in this case, you might never know how the professional hacker around the computer has done what they've done. But online inquiries are quite black and white. They're quite- there's always a trail to follow through, say, a computer network through a system, through a programme to follow that line of inquiry, to get to the other end. So, it's like, treat it like any other investigation. And you kind of can't go wrong.

AB

Yeah, no, that makes absolute sense. And I think that's the beauty of cyber as well and that you get a lot of people that that kind of start out in that kind of area. But they come from different backgrounds, they have different levels of expertise and it kind of- it creates this diversity of thought and I think that's a great thing. I wanted to ask you a little bit more about kind of cybercrime and what's meant by cybercrime. Would you be able to kind of touch upon that in a little bit more detail?

DT

Yeah. So, cybercrime, it's a bit of a catch all term for any kind of criminal activity that's carried out using computers using networks specifically. The Internet as a network to kind of widen the scope of that offending that criminal behaviour and to, you know, widen the impact. The criminals can get more out of it if there's a wider reach. What we tend to say though, is in the cybercrime unit, we deal with crimes that are legislated under the Computer Misuse Act. 1990 that act- well, as I say it’s from 1990. So, it was written in the late 80s and it was enshrined in law in 1990 when the Internet was more or less- it was around- but it was a concept. It wasn't a general thing so I'm quite impressed that we've got an act in law that was written back then but it's still relevant. And don't get me wrong, there are- There are some parts of it which we struggle with now, and the government are aware of that and some of it's currently looking at a review of the computer misuse act, just to catch up with the sheer advancement we've had in technology, but that act gives us things like unauthorised access to a computer system and its most basic level, so you're basic hacking taking over of accounts. Then it moves on to unauthorised access with intent to facilitate a separate offence. So, using that access to commit further offences. Up to things like unauthorised access with intent to impair a system, so your DDoS type stuff. your ransomware jobs, so it does cover a lot of the stuff that we see in today's world and…

AB

It's good, good little overview and snapshot and this kind of question naturally comes after. But the Home Office and the MoJ, the Ministry of Justice, refer to cyber enabled and cyber dependent types of crime. What do we more simply mean by these terms? Would you be able to break those down?

DT

Yeah, cyber enabled. Like you said, the kind of what I mentioned at the start of that last question, so here you'd look at. What I'd refer to as a traditional crime, so crimes that have always been there, your fraud, stalking, harassment. Multitudes of crimes. So, cyber enabled is that type of traditional crime where the scale, the reach, the impact is massively increased by the use of computers and the Internet. These can be any crimes like I said, but what we see a lot of particularly is fraud. I mean, fraudster sat behind the computer with the power of the Internet, there to send out a phishing link to 10s of thousands, maybe millions of people is going to clearly have a bigger reach of people clicking that link and coming back and then taking the money than a fraudster with a phone book and a landline telephone cold calling people. So cyber enabled just gives criminals power really to use cyber to commit traditional offences. Cyber dependent crime on the other hand, that is where you'd be using a computer or a computer network as the tool of attacks, or the vector of attack as well as the thing that's being attacked. So its a computer attacking a computer and it's legislated under what I just mentioned there the Computer Misuse Act. We refer the kind of split cyber dependent crime into categories, let’s say you’ve got illicit intrusions into network, so your Section 1 computing misuse act, that kind of stuff, the unauthorised access to a network to assist them and then disruption and downgrading computer functionality. So that's where you got your DDoS, your ransomware type attacks, where you literally are disrupting that computer so no one can use it. So kind of, we look at it in that way.

AB

Yeah. Thank you for that and in relation to the cybercrime unit and the kind of remit of work that you carry out. What does that look like? I know you're kind of under Lancashire Constabulary, but is the is the cybercrime unit something that's national and kind of what remit of work do you carry out?

DT

I’ll start off with Lancashire. A bit of an overview, we've got a relatively small cybercrime unit, most forces do. There's myself and we have 3 pursue officers, which I'll talk a bit more about in a sec and we have two protect prevent officers and again I'll mention protect and prevent and what they mean. So that's really our unit. However, UK law enforcement approach to cyber is that we have a connected national network so that we can share intelligence through the network we can give a consistent message to victims of cybercrime. Make sure that it's not a post code lottery wherever you are, you're going to be getting the same message in the same service throughout cybercrime. Just standardising it and professionalising really, how we how we deal with it. The government at the top have set out the UK's National Cyber strategy, which was updated and published this year, and that gave some- It's like the strategic level what they want the cyber landscape to look like and how they want law enforcement to enforce that. So that came out this year and that's brought into play with the National Cyber Crime Unit, who are part of the NCA they work with that, produce material to share across the network, which we can then obviously work with victims of cybercrime and potential future victims. So, we've got the NCA coming down from the government and then they feed into we have around the country, 10 regional crime units, regional organised crime units and they deal with all sorts of organised crime and obviously cybercrime sits within those regional units.

Here in Lancashire, we're part of the Northwest ROCU, we call it Northwest Regional Organised Crime. Units. We are one of the six NW police forces that are overseen, shall we say, by the Northwest region. And then we come down to our force level where we implement the strategy that's come from the top and we go out and we do the talks to the public, we speak to people. Again, that we split the office, or we split the network down into 4P's. We have this across a lot of law enforcement. We have to pursue, protect, prevent and prepare, so I mentioned we've got 3 pursue detectives in our office and their job is kind of what it says. It's pursuing the criminals, it's the investigation arm of the department. And they're concerned with the following lines of inquiry to trace any offender and potentially prosecute. As you can imagine cybercrimes, they're a borderless crime. It's not something that the criminals going to be in Lancashire and the victims going to be in Lancashire and we can interview, we can deal. It's it could be national, but more often not. It's international, so we don't always, not everything we do leads to prosecution. And that's where, as an old police officer head like myself, it took a bit of flipping around, shall we say. It's not about just catching the offenders, it's about, empowering people and businesses to protect themselves, make themselves more resilient.

Pursue. We do what we can to trace and we catch and the information we get even if it doesn't lead to a prosecution. Intelligence is fed back up the network, to national level and international partners and then that intelligence can be used to take down criminal groups all over the world. It often is so you might feel like we're not getting anywhere, but we do in the long run make a- make quite a big difference. So that's the pursue side, but unfortunately as I just kind of touched on there, it's impossible to arrest your way out of cybercrime. So there has to be a different way to deal with it, and that's where the so we say the protect strand comes in, what we're here doing today and what we're talking is raising awareness. But we do that both proactively in the police and reactively. So reactive protect is someone's already been a victim of cybercrime. They may have the as an individual maybe their social media is hacked or a business that could be a victim of a ransomware, but there's no lines of inquiries that we can follow. Or sometimes businesses don't want to go down the investigation route for many reasons. We feel we need that protect messaging so we'll go in and we'll sit down with them and we'll talk about how to make yourself more resilient, how to make yourself more secure. And it's not always complicated, technical things, sometimes the most simple advice can- passwords, for example, is the massive breach- simple advice can protect you for want of a better word. I kind of from my own mind, I always think of cyber-attacks and the advice that I gave in general terms and shall we say old-fashioned, for example passwords, people with weak passwords get breached. It happens and I'll say you don't go out your front door when you leave to go to work and leave your door unlocked. However, your stuff in your house can get stolen, but in an online digital world, you're leaving your front door i.e. your password, your access into your account insecure so that people can come in and take your data. So, we kind of that's the way I personally talk to people. It seems to come across well. Then we have the prevent strand. This is more offender focused and we work with people pre offending. Where it may be and it is a lot of time young teenagers, who are very clever on computers may not be getting challenged enough at school in the computing, so they kind of defer towards the darker side of the Internet, shall I say, and go on forums and learn about hacking. They might buy tools where they can DDoS the school just for- just for fun, and that happens quite a lot. So, we have a referral system where they come in to us and then we can work to kind of reeducate them a little bit and point them in the right direction to the to the better side of cyber, to working in the cyber security industry. We want to harness them skills they've got. We don't want to prosecute them, criminalise them and make it- It's all bad. Use them skills for positive, so we work with businesses, we work on the, we've got the cyber choices programme. Through the network that we can put these people on and work with them to realise that there's a massive cyber industry out there they can do this for good, even if they like hacking. You've got the ethical hacking side. There's so much out there and we want to show them that and that they can earn money rather than being arrested all the time and hiding from the law, can't they? So, there's that. And then finally really the prepare, which we mainly work within law enforcement, it's about upskilling Officers like I used to be. Didn't have a clue about cyber. But we're dealing with this day in, day out, and we're missing opportunities to help victims. So we do we train in with, you know, our staff and upskill them just to recognise, for example, we get a lot of domestic abuse related cyber stalking, harassment, might be putting spyware on victims computers and we need to train officers to recognise that and to deal with it because it's only getting more and more of this, it's not going away anywhere. You can bury your head in the sand however you want. But cyber is here to stay and it so yeah, that's how the network fits together.

AB

I know it's really, really interesting to see kind of what remit of work you undertake and the scope of that work. And I think the beauty of the work that you do is the collaborative element, of course, you know you support with the Lancashire Cyber Foundrys workshops, you deliver talks there for the businesses that we get in our programmes and it's great to hear the work that you're doing with younger people as well you mentioned earlier about attending kind of freshers fairs and it's that awareness element that I think is really, really important in this kind of line of work. I wanted to touch upon the cyber threat landscape. It would be good if you could kind of describe that in a little bit more detail based on the work that you do and it would be good to look into the general level of awareness amongst the population. Is there a lot of work to be done to educate and inform people of the severity and seriousness of cyber security?

DT

Yeah, I think no matter how aware people get, there's always going to be work to be done to educate and make them more aware because as we get better at protecting ourselves, what we inevitably see is criminals have to innovate to get better, to do what they want to do. So without trying to scare monger too much, I think the threat landscape as you mentioned there it's pretty severe. When you see what's going on around the world, we've got nation states have attacks all that a lot of attacks that we see ransomware for businesses for example, that are coming in, they can be traced back to Russia is a big one, a lot of Eastern Europe. And these attacks, some of them, are believed to be state sponsored and then go on to fund other things cause there's so much money being made in attacking and when you think state sponsored Russian hackers are not going for always big national critical infrastructure, they're going for sometimes small medium businesses where they can extort money out of them and doing that over a wide scale over the world they make millions and millions of pounds so it's something that's never going to go away that side of it. We do also like I say get attacks on- this is where the government are taking the threat landscape seriously and we have the obviously cyber force coming up to the northwest soon. And we have this cyber strategy because they are saying that if you want if you want to be attacked by an external power shall we say using cyber to close down your national infrastructure can bring the country to a standstill, can’t it? So, it's quite a scary place to be at that side of it. When you mentioned knowledge and awareness, yes, it is always increasing, but like I said at the beginning, the risk increases too. Personal data, I think is probably one of the most valuable commodities we have nowadays for so many reasons. As I imagine you can understand, and people know that and they want to get hold of it and criminals will do whatever they can. We've seen a rise in breaches over the last couple of years with businesses having staff working at home for out COVID, for example, they had to change their working practises very quickly and come up with new ways to work and that was work from home and some of them. Yes, you understand why, but speed was more important than getting security, right? So, we had a mass of breaches of remote desktop protocol in Windows, for example, and firewalls and VPNs that weren't set up properly. It was- It was great for criminals, and now we're getting kind of over that and we're working to get that kind of stuff sorted, but they move on to the next the next big thing. And again, I said awareness. There's always going to be work to educate people and I think it's people's awareness has massively increased over the last few years, particularly the younger demographic who have grown up using the Internet. They've grown up using devices and their whole life is spent on a device. So yes, they've got really good awareness and education around the devices. However, that doesn't make them secure on the devices they want data quickly, they have multi factor authentication, 2 factor authentication. They can't- Sometimes we see you can't be bothered waiting for a text to come to my phone I just want to log in now so we see the younger demographic. It is kind of. I want it and I want it now so. They're skipping security for speed.

AB

Such short-term kind of thinking and logic isn't?

DT

It is so, yeah. It's so where- what I'm trying to. Yeah, yeah. And what I'm trying to say is awareness doesn't always lead to being more secure. Yeah, just the two FA alone that having that set up on a device can cut out 90% we think this that is of just basic unauthorised takeover of accounts. You just become a bit too blasé and not just that. It's about what they share, what people are sharing online. You want to share your whole life and you want to show everyone exactly what you're doing. But that can have massive ramifications. So yeah, there's definitely work there to educate the younger. People, but take the next generation on, the older people who didn't grow up with the Internet may not be technically minded and probably count myself in this until I came into this arena. They might lack the confidence to safely use the Internet, but on the other hand, their security is higher because they're scared of being attacked from all different angles, so they may be more secure, but they just need to learn that not everyone's bad on the Internet. Not everyone's out to get you. So there’s different--

AB

balance in factoring in kind of different levels of experience of using the Internet like you said.

DT

And that's kind of what we find about the threat landscape. It's getting the right message to the right people at the right time really-

AB

- and tailoring it.

No, that's perfect. And in your experience, is there a reoccurring theme or pattern in relation to cyber-attacks on businesses more specifically. A common denominator, perhaps with a consistent theme and for our listeners tuning in, would you be able to provide us with a few examples or case studies that you may have in relation to kind of cybercrime?

DT

So, a reoccurring theme. Like I said we do we get- We get all sorts and things like the big things ransomware, extortion through that exfiltrating data and trying to sell it back. That's never going to go away, but that's not always the main thing we see. I think the main risk to businesses, especially small to medium businesses, are what I would describe as relatively low skilled cyber-attacks. So here we're talking about main breaches coming from phishing links sent via emails or text, and what we refer to as insider threats, so staff and by inside of threat I don't mean just malicious. There's staff may not be trained to do something properly that.

AB

Yeah, it's kind of unintentional.

DT

Yeah unintentional.

And like I said these don't always take what you'd imagine to be the stereotypical hacker sat in a dark room with a hoodie on the Internet. You know, using all their tools, all their skills to breach a network, fighting against the defence, that kind of thing, all dramatic, it can take a teenager in a bedroom who's bought some, breached it a password, for example. And trying these passwords and accounts now, that's how we see a lot of individual social media accounts being taken over, that its come from a breach from a potentially a previous ransomware that day has been out on the Internet, it's been purchase. And people's password security, so I've got the same password for my e-mail as I have for my Facebook, my Instagram, my social media account. So once they're in your e-mail, they know what accounts you can have they move laterally across all your accounts and take over. And that doesn't take cyber skills and that kind of blew my mind when I came into the industry, shall we say, but that's one of the biggest threats we have. And the same for businesses, weak passwords, poor account management, not removing staff from accounts after they've left the company and just staff limited staff awareness around the security. And I'm not saying it sounds like I'm getting at businesses here, but I'm just this is what we kind of see and the simple things that they can change to. I've used the word few times but empower themselves to make themselves more resilient to these kind of basic attacks. Now what we do see is that even businesses that will be non-technological or not a digital business, it may be a small 2-3 person operation where they have a social media account might be their only Internet facing device. But if we try and get the message across- Because if they lose that access to that account, that could be fatal to their business in the long run. I've always said to people that Hackers and cyber criminals, like all other criminals out there, are inherently lazy. They don't want to do the hard thing. They want to get your data and they want to do it in an easy way. So phishing and like I said, staff limited awareness inside of threats, that's their way into the into the system. So, when I mention phishing attacks, we see problems- Most of the small businesses that get attacked around us are from that, and that could be, like you said, you want some case study examples. We’d had an incident recently where it's actually in Lancaster, an estate agent was Victim of attack. Well, they weren't the victim as such, they'd be approached by some of their potential tenants who had been in touch with them, saying we've given money across, but we've not seen the house, W-what's happening? And the estate agent said that we haven't got that far yet you were talking to us. We were looking for property. We haven't found some. So we've gone into the systems and realised that a third party has taken over the E-mail account of the business and been messaging out to clients who were already in the process of asking for properties to Send money urgently because this house is going to go and you really need this house. You must secure this senders, for example £500.

AB

Secure. Kind of, yeah.

DT

Now I think it was four or five different victims of that so when we took a step back and looked at it. It was from a simple phishing link to the reception computer, had come in now what the hackers for want of a better word, The criminals, have done is they've gone to the national site Zoopla right move where they can put a message to all local estate agents in, say, the Lancaster area. I'm looking for a house to rent for six months, I've got the money upfront, Please send me details, here's an e-mail address, and it's just a burner e-mail address, a throwaway e-mail address, the person working the estate agent has then gone to- sent an e-mail back to this address saying yeah, we've got a lot of we've got such houses. Send us some further information and we'll get back to you. Hackers then replied back to that estate agent with a link saying here's my CV, this is what I'm looking for, please click here. So the person's clicked as it would it's CV, They said they receive these things through all the time. It says it's a PDF document, but it went to an Office 365 sign in Page so she thought she'd been logged out of her office 365 put username and password in, Still wasn't working, so I kind of gave up on it and said oh, that didn't work. And sent a message back to the person saying please can you send your CV again we- the link doesn't work and then never heard anything back. Having those credentials has then allowed this third party to log into the system, look through the emails, find out who was looking for houses, and then obviously go through.

AB

Kind of access to that database and then being able to connect to the people.

DT

So yeah, and so the way I looked at this is one business in Lancaster, it's come from a national site. I've got no doubt whatsoever this is going on all over the country. And the person I spoke to, for example at the stage and said how stupid doing that, but I try and get that across it's not about you being stupid. These are professionals that use social engineering techniques to get what they want from you and. It's not your fault. This is what they do for a living. They will get it one way or another, and kind of- So that's kind of an example of how we see a lot of phishing attacks coming through like a real world example of what happens there. And then as I said, that's grown from a one-shot being attacked through to potentially national type organised criminal group doing this and that's not just one industry that happens across all.

AB

It's kind of like they understand the climate in which businesses operate as well, don't they? And then, of course, victims kind of fall for that, which is a real, real shame. One of the things that I wanted to ask you was about the kind of trajectory as well of cyber crime, I know that Action Fraud kind of have a role to play in that. Would you be able to kind of just briefly touch upon how cybercrimes get dealt with via kind of the cybercrime unit and what's the kind of trajectory for say, for instance business owners that get attacked, what is their next kind of call to action?

DT

Yes, so, start off with actual fraud, so actual fraud aren’t an investigation body. They don't deal with investigations; they are a national reporting body. They are the reporting body for all fraud and cybercrime, so they'd receive all the reports, collate these. They look for patterns. They look for intelligence and they look for links to other kind of crimes and they'll feed that into the national networks or, it builds that national strategy, but then they will disseminate the report to the appropriate law enforcement body to deal. So, if we have a victim in Lancashire, for example, it would come back to Lancashire force Cyber Crime unit to do the investigation, to deal with the victim moving forward. So some people do think action fraud are investigative body, but they are generally collecting it and that's where cybercrime differs from traditional crime. If you were a victim of your house being broken into, for example, you would ring the police. The police would be your first port of call. You would go to them. And this is the message we're trying to get out about cybercrime. When you're in the police, the controlling operators are trained to say to people if it's a non-ongoing, I'll get to the urgent sales in the threat in a minute a business has been live attacked by ransomware and clearly you're going to phone the police and get that response straight away. But coming after the weekend and something's happened, your first reporting body is action fraud and then we get disseminated back to the police. Now the reason they've done that is because that does build up that national picture and it helps with crime recording stats. We know kind of trends in cybercrime, what's happening and it is working and we do see a more national picture. Sorry, I think your second party question was around what would businesses?

AB

What would their next call to action be in the instance of kind of following, maybe if they reach out to action fraud, disseminated back to you guys. You know who picks it up?

DT

Any cyber dependent crime as we talked about before that would be picked up in my office. So we would decide if that was a protect or a pursue investigation. So if it's going to be lines of inquiry. And we're always victim focused, especially when it comes to businesses because for many reasons. So we there's a stat I think over 80% of British businesses have been subject to a breach and that was 2020/21 and that's stats that have come from the National fraud intelligence bureaus made from these action fraud reports and they think that's massively underreported. So there's legal grounds that businesses have to report cybercrime obviously, the Information Commissioners office for GDPR and that kind of stuff. But they don't always want to investigating, and I understand that as a business, there's all sorts of reasons why and cyber criminals obviously play on that as well. So we get a lot of ransom notes to businesses when they've had their data encrypted. Part of it will be don't contact the police or the feds or something they usually say because they will come in, they will seize your computers. They will stop you working. We, the cyber criminals, have found this vulnerability and we're here to help you pay us a small price will give you data back, but if you go to the law enforcement, obviously they'll be a bigger price because you could lose your business. And I try and put myself in position, If I was a business owner, it it's scary, isn't it? It's your whole livelihood, your whole world. And if you stand to lose that, then paying a smaller fee might help get the money back. We always advise not to pay because they have got your data. They have been in your system. You don't know if they're still there, for example, or what they're going to do with that data later. Numerous times you pay, you get your data back. A few months later, customer records, Personal identifiable information starts to be on the Internet and they use that second strand to extort you. So, I'd say they should report it to us and we will work with you for the best outcome for yourselves and most of the time, that turns out to be we'll go in and we'll work with staff training. We'll sit down and we'll do the protect meshing around phishing links around inside of threats, around raising awareness passwords, updating computers, multi factor authentication. Just giving that- what can be really basic advice which can make you less attractive target to a criminal. We obviously also have places like yourself. Working with doing a great job with small businesses in the area and the cyber resilience centres. Which are government funded organisations around the country where businesses can go to for that extra training. They do tabletop exercises, they come out, they for I think there's a there is a small fee for part of the subscription. That there's a free advice, place and as a subscription they come and they have instant response teams who will come after attack and help. So there's so many people out there to help you, but we need- we need to do a better job of getting the messaging out what needs done and kind of that's why we're here today.

AB

I think, yeah, absolutely. Our last kind of guest speaker, Paul Vlissidis, who featured on the podcast. He mentioned a point about kind of cybersecurity being inextricably linked with businesses in today's world. I was going to ask you if you agreed with that, but it would seem as if you do. And it's a similar type of message and I think that's one that I agree with too. I wanted to ask about kind of cybersecurity and the future of cyber security and how you see that kind of unfolding.

DT

Cyber security is always going to be needed. And as I mentioned it before that with greater awareness comes a greater threat because criminals, often have to innovative more to get our data. So there's always going to be need for security and things that might seem newer or unnecessary to businesses now, like we've seen a lot of businesses getting cyber insurance. This is a new thing that's come in the last few years. And I don't need that, that's not for my business. So, it's something that's just come out, it's new or even having an incident response plan for any cyber instance or business continuity plan, what would your business do if you were subject to a cyber-attack and you lost all your network, you lost your computers. We use a lot of online voice phone type systems, you lose all your phones, all your customers, what would you do as a business if that happened to you? and most a lot of businesses don't have that. “I have never thought about that, how would I carry on trading if I if I lost that?” So, what I'm saying is things that kind of seem new or maybe unnecessary now I think as the future goes on, these are going to become the norm. We have normal insurance for all sorts of different things. Cyber insurance is just unfortunately going to become part of the landscape, awareness training just everything we've talked about before is just going to become normal rather than specialist. I think cyber security is seen still as s bit of a real specialism, but and I don’t class myself as a cybersecurity expert, but working in the cyber field and learning so much in a short period of time, I think if people like me can get involved in it and do it, it opens it up for so much. So, it doesn't have to be so niche, so expert so kind of kept to ourselves. It needs to be opened up and kind of that's what I'm here to shout about. That awareness and building awareness really.

AB

Yeah, absolutely. It'll become one of those kind of key considerations like we see with many other things. So I agree with that and what's an ideal outcome for you and the cybercrime unit, particularly in relation to the work you do across Lancashire?

DT

So, I've mentioned a couple of times for me as a police officer, my ideal outcome used to be getting what's best for victim, getting a conviction, catching criminals, catching bad guys and dealing with them. And I've had to change my thinking a lot in the cyber world because, yes, I'd love to catch everybody who commits a cyber-attack, but let's just face it, it's not always feasible because of the reason talked about it, its all over the world.

So for me the ideal outcome for us is just to raise that awareness for people, make them more resilient, get them to protect themselves online and not bury their head in the sand, make them less attractive to criminals. So we're getting less cyber-attacks across Lancashire. People are more confident in using online equipment, understanding the threat landscape that we've talked about. That's probably what I think is the ideal outcome. And like I said earlier, someone did once say to me you can't arrest you out of cybercrime and I kind of like that quote and that's stuck with me. Helps me say that when I when I push this messaging out there also another good outcome is that people- just raising awareness helps people think about what they're putting out there on the Internet. So we give advice in our national network from the National Cybersecurity Centre, the NCSC, which is a brilliant website, government website. Which breaks down for individual small businesses, large businesses and has really good basic advice on how to keep yourself safe online. So, everything I do always feeds back to that and if I talk to someone, “Just go and have a look at that, see if you can learn and learn anything.” So...

AB

Yeah. No, that makes absolute sense. And I think you know you've touched upon the different areas of support alongside kind of the work that you do and if and that's as long as that continues, I think that we will eventually start to see a point where hopefully those statistics come down and we do see a kind of more securer future, for whether that be online business and an online way of doing things. And I think a nice way to finish here is to kind of touch upon, you know, the advice that you would give to others wanting to enter the sector. There is a lot of opportunity within the cyber field, you know we see that at board level within businesses. You know you have cyber security leaders that are helping steer the ship from a cyber angle, through to academics within higher education institutes that are shaping policy and pumping out research and then of course you have teams and individuals like yourself that are raising awareness and you know are actively investigating cybercrime and it's all forming a great part of this kind of wider ecosystem which is very exciting. What advice would you give to those that are wanting to kind of enter this particular sector?

DT

Yeah. So I feel like as a police officer can be a bit negative and I've might have made things sound a bit like all doom and gloom, but it's definitely not like that. And this is a really exciting and ever evolving sector to work in. Nothing's ever the same. I've not been for that long and I've already seen changes happening as technology improves and we do things in different ways, so anyone who's already thinking about it, there's no reason not to. Doesn't matter if I've touched on it a few times, doesn't matter if you're not technically gifted, if you're not technically minded, there's a job out there for you for everything from the social engineering side of the job, up to the- we have businesses just set up around given the advice, so you don't have to be technical. It's just having that love of cyber or that wanting to help people. That's the way I look at it. And then the other side of it, if you've got the… you, you're technologically minded, you know you've had formal qualifications, computer science, so many different degrees, educational routes. Again, you do a lot of them yourselves at Lancaster University for Cyber in General Cyber Masters. Everythings out there. Do it, there's nothing holding you back. It's such a like I said it again, an exciting industry to work in and people do roll your eyes “Cyber exciting” Do they- Do they go in the same sentence? But I think so. And as the world becomes more digital, as the Internet is changing as we have cryptocurrency of all sorts of things out there, there's so many niche areas you can go into, so there's nothing to hold people back. One thing we are pushing at the minute in law enforcement and across our whole national Cyber Network is working with neurodiverse people. You know, get them into the network because people with neurodiverse traits, they may think in a different way to someone who hasn't got these kinds of traits, but kind of in the last few years it might be looked at as that's a negative thing, but it should never be looked at as a negative thing, because especially the problem solving we have to do in cyber coming at that from a completely different angle- not this structured rigid way, this is the this is the way it's done- It doesn't work like that, and especially these problems need solving from outside and a lot of business have got involved in that and where you we're seeing it in cyber as well. And these are the kids in the prevent network that we want to work with because they do, they are- some people are so good at computers, but might not be great at other parts of school or might not be getting challenged at school and we want to catch them before they do the wrong thing and use them skills and utilising the industry. So there's a massive gap in the industry for people who are creative thinkers, and that's the biggest thing for me.

AB

I think that's perfect. Thank you so much Dave for your time and for agreeing to be part of the Demystifying Cyber podcast. It's been a pleasure. So, thank you.

DT

Thanks for having me.

AB

Thank you for listening to the Demystifying Cyber podcast. We hope you've enjoyed today's episode. Feel free to get in touch to find out more about the Lancashire Cyber Foundry. Join us next time to further unpack and demystify the cyber landscape.