

ABSTRACT SECURITY

Date: 19.09.2020.

Interviews with: Freaky Clown (FC)

NoMan29: Hello everyone! Today we are joined by incredible FreakyClown!

FreakyClown:Hi everyone!

N: How are you? i hope you are doing fine !

FC: Busy as normal, but taking a break to sit down with you all here this evening.

N: I am glad to hear that. Shall we start with the questions?

FC: is that the first question?

N: Hah no but this is, can you introduce yourself for the benefit of those reading who might not know who you are.

FC:Sure, my name is FC and i am the Co-Founder and Co-CEO of a cyber security consultancy called Cygenta based in the UK (www.cygenta.co.uk or blog.cygenta.co.uk). I have been in cyber security for as long as it has been an industry, about 25ish years! I have been a senior penetration tester, head of physical assessments, head of socail engineering and until i strated Cygenta with my wife (dr Jessica Barker) i was the head of offensive cyber research for Raython.

N: Oh wow, that is impresive! so your job involves Cyber and Physical security.

FC: My job involves mostly running a company day to day, but i still get involved with the technical and physical jobs when i can. My wife covers the side of securirty which is the human element.

N: Oh nice so you have that sorted out. And how did you get into Security ?

FC: Well that is a long story. Back before ther ewas an industry, i was messing around with tech, i was active on BBS systems and gaining access to modems around the world. ONce the world wide web was invented i soon shifted over to exploring that and quickly god a job being a sysadmin for a small local tech firm. From there it was obvious who had to deal with the securirty aspects, so very quickly i moved into simulated attacks against our company to help figure things out and set up defences better. Not long after that i moved into ethical hacking full time and gave up sys admin work and defences work entirely.

N: Wow that is pretty interesting story. But i have to bring us to the present time. How has the pandemic affected your work?

FC: It really hasn`t that much tbh, a lot of our clients are giant global companies and most of that work was remote. We were fortunate enough to

have a lot of work speaking and therefore traveling alot, taht side has stopped for now at least. But the main work has remained steady and similar. Our entire team was working from home anyway and so nothing had to change in the aspect either.

N: That is nice to hear that your work didn`t stopped.

FC: we were fortunate that our initial ideas of how to set up and run the company paid off!

N: But i belive that physec did slowed down a bit?

FC: Many companies we know unfortunatly went under very quckly because they could not adapt fast enough.

N: Yeah taht is very unfortunate.

FC: A little yes, but not so much imho. Maybe our clients are different to others.Global banks tend not to stop for anything (even if they wanted to). Foreign physical security assessments have slowed that is true though but mostly because we can`t physically get there!

N: Yeah understandable.

FC: We have a physical test of an Oil Rig that has been postponed until we can get there.

N: Ok now this questions you got a million times i think. WHich skills does someone need to be successful at physical penetration testing? - I terms of skills.

FC: Well the obvious answer is basically, learn to be confident, but not an asshole samramy confident. Quietly confidet! Observation is another, knowing what to do when and where is key to success in a lot of things not just physical tests. ALso, be kind, never go in pretending to be very angry or somthings, humans like to be liked. But thats a general life rule, try to give back as much as you can and be kind to one another. People are dealing with things you have no idea about and we all just want to get on with our lives.

N: Yeah to understand other side too. Some people just get to technical stuff like you need to learn this this and this.

FC: ergh technical anyone can learn, it doesn`t take much. But the mindset is where you need to focus your efforts,

N: Yeah i agree.

FC:Focus on the tool and you will be outdated, focus on the why and you will be able to use any tool!

N: Nicely said! What set of skills you look for when hiring soemone ?

FC: we don't, we look at the person and their outlook and how they behave etc.. One guy on our team was a welder before joining us for example. We also don't bound people to a role, we bring them in and we give them the tools and time to learn anything they wish, that same guy he was brought on for a technical role. He was able to spend more time learning his hobby and we just moved him into a role producing videos for us insted.

N: Huh that is interesting. This is the first time i heard something like that and i like it !

FC: we want to help people grow. We want to give people everything they need, skills and time etc in order to make them good enough to move where ever they want to, even to another company! But we hope to make working with us so enjoyable they never want to leave.

N:Ok i must admit that this is really phenomenal! It is innovated and i like it! What is the favorite part of your work and what is your least favorite?

FC: Favourite, is seeing the difference we make to a company. Seeing how they are when they first call us to when we finish work with them and they see the benefit we have brought them! The other side of the company that i haven't spoken about is our outreach. We do a phenomenal amount of outreach to kids and universities and that side is really amazing to me. It's what i wish i had gotten when i was a kid, so making an impact on kids to turn their lives around is a core part of Cygenta. In fact you asked earlier what we look for in people... it is that drive to give back. Everyone at Cygenta does outreach. Not because they need to but because they want to. We have a young lady Madeline, this is a director of Cynam in Cheltenham, we are also partners with the NCSC as part of their schools hub program which we are heads of too. We also work closely with TeenTech, a charity to get more kids involved in STEAM jobs. We give over one day a week of Madeline's time to help run those projects with the NCSC and we love doing things like this, giving back to the tech communities to share knowledge etc with them as much as we can. Mate hated...writing proposals (it used to be reports till i started running a company).
www.cyberhub.uk and this is the NCSC project i mentioned
www.teentech.com.

N: Your company is really amazing ! I am glad that i am speaking to the person who is giving to community and who is trying to educate many people ! So what would you say is the biggest success in your career? Cygenta?

FC: We spoke to 6000 kids last year alone. By far Cygenta is beyond anything i could have imagined as a kid growing up with nothing. We are fortunate enough to be guest curators of Cheltenham Science festival a few years ago and that saw more than 10,000 kids in a week come through and learn about science. www.cheltenhamfestivals.com/science/
It is Cygenta and our awesome team that keeps that keep[s things going that allows myself and Jess to get out and be the face of things like that. So i am very grateful to them all!

N: I am very glad to hear that! Now next question is which resources do you recommend for Physical Security ?

FC: mmm thats a tough one, you can't really learn it online, only the theory. It's like learning to swim by watching youtube videos (that is literally what i did btw). But at some point you're going to have to just do it! (just do it is a trademark of Nike and not affiliated with me).

N: hah ok i understand, at some point you have to try stuff. Not just learn and read. What for someone who is just starting to learn about PhySec, what would you recommend ?

FC: tbh the biggest resources that i know is this place. I heard great things about it and thats why i agreed to take a part in the interview. I think the community around physec is growing and it shows that places such as this are needed. So thank you for getting this rolling and letting people learn from one another . Talking to people, networking and not being a dick are all skills you need to do physec so what better place to learn that then in a community of likeminded people?

N: Ok let`s be clear this is not scripted so people don`t think this is some kind of paid advertising (i will wire you later your 50\$)

FC: Hahaha. When i was growing up, i learnt things by either experimenting or by talking to other interested in the art of hacking. Places like 2600 and such really helped. Like wish for physec and here.

N: Thank you for this, i am still a student and a person who wants to learn so that is why i made this and i hope it will help someone!

FC: That is the best way! Often i see people who complain that such and such isn't near me....wellll take the initiative and start it! When i moved to the cotsworld, there was no DefCon goroup, so i helped started one. People like to help people that are trying. Like imagine you saw a car broken down on the side of the road..no one stops.. but if you see someone pushing thier car, people will stop and help. Dont complain DO somthing and others will help you!

N: Hah that is very good example! Next question is Can you explain some examples of how the USA and European security awareness is different on a practical level? Of course there is a lot to talk about, but what are the key differences?

FC: Well we are very fortunate to trancel the globe and see security from a ton of different perspectives. How conutries handle it and focus on it (or not) varies wildly. You have to understand the history and culture of a country before you can rush in and do it your way. Let`s take a few examples. Scandinavian coutries have what is known as the Jute rule. It is an ancientish cultural thing that basically means no one is better than anyone else. A noble and lovely thing. But that means you can't ever position yourself as an expert! Asian countries tend to be the opposite, lead from the top down. You need to show you are the world leader! How you react in certain countries for example also needs to change. In

England if you are stopped on a SE job, becoming confrontational will make the stopper reconsider, but in America that wouldn't work, they would counter that by being confrontational themselves. There are many examples, but they tend to all border on semi offensive broad sweeping comments. I mean no offence to anyone obviously! Countries have cultural differences, but companies and clients can be very similar across the globe no matter where they are.

N: Yeah, i agree completely. This kinda goes with the next question: Many countries with less developed security industries suffer from social engineering attacks, which cost them a lot of money. Nevertheless, a common argument given is that there are many other issues that need to be addressed before social engineering attacks. How would you respond to this argument?

FC: Crims are going to crim, they will always target the weakest point in order to get money or data. When you get to the point you have something that is valuable, you should be doing something to protect it. There are bigger issues to be solved yes, but protecting what you have is vital. We give presentations on all sort of nationstate style attacks, because that's when it is in the media and that's what people are scared of and they want advice on them. But we always end it with the advice that even nation state hackers will try the simplest and cheapest method first. When i was doing offensive cyber research for a defence firm...you know the ones that perform kinetic style attacks? Well we would always weigh up the cost of development of cyber weapons over just dropping bombs. That is what criminals do.. they don't but the 100,000\$ zero day to get into random persons account, they send a spearphishing email to 20 million accounts and get a huge return on investment of time and money.

N: Yes i agree. Most governments spend on all sorts of defenses but they forget to defend from simpler methods that are mostly used. Now something that doesn't reach to politics. Do you look at Physical Security more as art or science?

FC: It is fantastic blend of both, like flying a kite or windsurfing. There is science behind it but at the end of the day you're trusting your gut instincts and working with experience to get the result you need.

N: It is a bit of both. Ok now something career wise, in your opinion, which is more important, having relevant certs, or knowing right people ?

FC: The right people always! I have had very few educational certs in my life, i never went to uni etc. But weirdly timed and i promise not a loaded question but yesterday i sat and passed my CSTM exam. Not because i needed it but i wanted to check the training being given to our staff was to the right standard. People will always be the key to what you do.

N: Yeah but many companies want that you have paper for your knowledge.

FC: It all comes back to being nice, network and talk to people. There was a guy i met at a linux group i used to be part of, ten years after he messaged me with a question and has ended up being one of our biggest

clients. If company is demanding certs, they maybe need them. But that doesn't mean you need to have them to work and have a happy life!

N: Ok and now let's make you struggle a bit, which is more important today, digital or physical (including human security) aspect of security?

FC: No struggle at all! It is the reason Cygenta was formed.. You can not have true cyber risk management unless you understand that all three of those areas are needed and they need to wrk together! Cygenta was formed to enable us to help organisations to achive that. Many many times i have seen companies spend tens of millions on digital security, only to have me walk in and literally pick up and walk out with kit that they were not protecting. Or physically security but uneducated in cyber crime and so susceptible to simple phishing. All three MUST work together or you don't have security, period. It's like upgrading your car to have big engine and forgetting that brakes are needed... and then forgetting that tires are really vital to both the engine power and the brakes stopping.

N: Hah very diplomatic answer, but i agree. Can you tell us, of many things you do in your job, which one makes your heart beat fastest?

FC: running

N: haha

FC: Ok so whilst that is probably true, i should answer it in the way it was intended.

N: It is getting a root shell on a machine, it will always be the most amazing to me. It is the end of a puzzle, the final piece. I have never highfived anyone over anything else in my job except landing massive contract i guess.

N: Ok and what is the one question you wished someone would have asked you, but never did?

FC: Great question, and one i am trying to work out a nice answer to....``will you accept this million \$ as a gift?``

N: haha

FC: ok a bit unfair i know, but i think the question i would really like people too ask me when i meet them is ``what can i do to help you help people more ?`` I go out to schools and talk to kids all the time.. and maybe once every 6 months i meet one kid, that one that is just on the cusp of becoming a criminal or has just started that life. And showing them the path they can take and help them get there is much much much more valuable to that kid than say buying million laptops to give to schools. Money doesn't buy the things we need to be doing as people. Money just makes people bitter and selfish (mostly). That is whi i take a minimal wage at my job, because i want the money to go to employees and outreach as does my wife.

N: As we are reaching to the end of our interview i want to ask you this, Can you tell us about the book - Confident Cyber Security: How to Get Started in Cyber Security and Futureproof your career ?

FC: Yes i can! So about a year ago my wife was approached to write a book to fit in a series of ``confident...``. Her subject matter is cyber security. So she wrote the book and its just been relased on the work and was a nuber 1 best seller in cyber security on Amazon for several days! You can read more about it here www.confidentcyber.com .

N: and my last quesiton is where can people find you ?

FC: Well the twitter is the best place to be honest. @Freakyclown

N: now let`s see if anyone else has questions for you... hey what is a ``usual`` talk a school like? (background, i work as a sysadmin at trust of schools in surrey)

FC: well it is nosy for one.. but the subject matter is what i do for a living. Its always around getting the students (and teachers tbh) to understand that this career path even exists. We had one girl contact us that her teacher and other students had laughed at her when she said she wants to be hacker ! How awful is that!? So we go in and educate eeryone that this is a safe, stable, fantastic and fun job that is legal and pays very well!!

N: Ok, what is the wierdest thing you have seen on a job?

FC: Oh wow, how to put this... So was years ago, i was pentesting a companies website with some others, and we found some saucy pictures of a girl hidden on the site. We found it very odd so we called a meeting with the client and explained what we found. He called in the techy saying he knows who was probably responsible. Turns out the techy web master had an interest in taking photos of his girlfrined and he hosted them on the website. He proceeded to ask us if we wanted more. That was very distrubing and weird !

N: Oh wow,... ok next one is if you could pick one cert to focus on to get you foot in the door, which one would it be?

FC: tbh pick the one that is going to get you into the company you want ot work for. Also go for the easy ones not just hard ones. WHY go straight to OSCP for example when you might not need to?

N: Why pigeons?

FC: So two things really, i blame my mate n0x, we used to sit around his hacking through the night and drinking cream soda, and putting pigeons into reports to show code being run. And what influenced that was a UK tv show called the phone jacker.

N: What is the easiest, walk in and out job you have seen?

FC: Ah that is easy, a client wanted us to get access to 4 folders. That was it, i walked in and few minutes later walked out with the folders.

END