EXCLUSIVE INTERVIEW WITH PAUL LOPEZ

Managing Director of the Eastern Cyber Resilience Centre

01 **Tell us about your background and experience in cyber security and how you got into the ECRC.**

I was for 27 years in the Essex Police as a Career Detective working predominantly in Serious and Organised Crime and Homicide Investigation – working as a Senior Investigative Officerin both disciplines.

I headed the Essex Police Online Team (POLIT) in 2015/6 tackling the growing threat posed by sex offenders operating on the internet. I was the Head of Serious and Organised Crime until 2019 where the use of crypto by top level criminals was starting to emerge. In 2020 I was appointed as the Regional Head of the Cybercrime Unit and in May 2021 I set up the Eastern Cyber Resilience Centre as Managing Director. The reason that the role appealed to me was that it was clear that the police could not arrest their way out of the threat posed by cybercrime and that a more proactive approach was needed, through education and awareness - helping businesses understand the need for cyber security and offering support and guidance to those who were trying to achieve it. Over the past 3 years, I have developed a good understanding of the cyber issues facing businesses, individuals and the public sector at a strategic level.

02 **What would be some cost-effective measures that SMEs could take to prevent cyber-attacks (such as phishing and social engineering attacks)?**

Nothing can prevent a cyber attack completely, so accept that you will almost certainly become a victim of a cybercrime at some point. Join your regional Cyber Resilience Centre, which is free and get enrolled on our Little Steps programme – a series of weekly emails, looking at bite-sized practical information to help businesses understand and build cyber resilience. Consider becoming Cyber Essentials accredited – this costs a few hundred pounds and is a Cyber MOT (a safety check) for your business – it comes with 20 thousand pounds worth of cyber insurance and reduces the likelihood of an attack by as much as 60% (NCSC and IASME figures). The CRC can recommend companies to do this for you. Contact the CRC about Security Awareness Training for your staff – trained staff are less likely to fall victim to a phishing email and to have stronger, more secure passwords. The CRC can also help with getting access to the Police Protect teams in your area – they can offer a number of free services to support your organisation.

03

How could an SME respond to a cyber-attack (best practices to follow post-attack)?

Don't wait till it happens but prepare for the attack before it happens and practise what your company should do in response to a cyber incident. Essentially – if you suspect a cyber attack, report it to your senior managers and IT support as soon as possible and disconnect the device that is affected from the network straight away. Make sure that you have some form of insurance policy to cover a cyber attack – if you don't, it could cost thousands of pounds to put right.

04

How do you forecast the future trend of cyber threats in the next 10 years? What would be the major drivers for the increasing/decreasing trend of cyber-attacks? (Especially for SMEs)?

Cybercrime is growing year on year and has shown no signs of slowing down. Expect increased accessibility to the tools needed to commit a cyber-attack. Basically, anyone will be able to carry out successful attacks in the years ahead, it won't need special skills or training, as the ability to use AI and off the shelf cybercrime solutions become more available. The automated nature of more cyber attacks using botnets means that criminals can simply fire and forget their attacks and conduct multiple attacks simultaneously.

The growth of the use of the internet of things (IoT), specifically internet enabled devices, has created new attack vectors for criminals – things like printers, desk phones and even air conditioning units have been targeted by criminals to access networks covertly ahead of them carrying out surveillance and then outright attacks. The ongoing trend in remote and flexible working continues to create additional opportunities for criminals who exploit weak router passwords and the fact that staff are simply more vulnerable when they are not geolocated with colleagues.

Malicious actors aren't just targeting large corporations, which is often what we see make the news. They are targeting SMEs as well, which they may deem an easier target because they often don't have robust tools for threat detection and to guard against attacks.

According to Forbes, in 2022, 30% of SMEs were victims of at least one cyber attack, whereas only 18% of SMEs were implementing basic security measures. One of the solutions is for SME business owners to increase their prioritisation of cyber resilience and to start viewing security as a necessary business expense. This means investing in tools and training that can help keep their organisation, customers and keep data safe.

05

What is your opinion on the impact which AI could have on cyber threats?

AI can be a force for both positive and negative in the cyber world; whether they cancel one another out is something that only the future will reveal. Looking at the negative side first, AI can be used to write malware as demonstrated by one user in March 2023, who used ChatGPT to write malware using Python script. Anyone can access malware through this method. A Zdnet report in 2023 showed that AI password crackers could crack 51% of passwords in less than a minute and 71% in less than a day. As computing power increases, this will only get better in the years to come.

AI has been shown to write very high-quality persuasive phishing emails that look and feel like the real thing. So, AI can even assist in the social engineering area of cybercrime. AI can be used to analyse stolen data so that criminals don't have to waste time sifting through millions of lines of worthless material. Less time doing this means more time planning and conducting fresh cyber-attacks. Though there is no direct evidence of this happening yet, it is entirely possible that AI could be used to look for and find software vulnerabilities – often referred to as 'bug hunting'. Finding these new so-called 'Zero Day' vulnerabilities would be very lucrative and could offer criminals the opportunities to access hitherto secure networks in order to carry out their nefarious activities.