EXCLUSIVE INTERVIEW WITH CHEN TSUI

Cyber Prevent & Protect Officer, Serious Fraud and Cyber Unit, Hertfordshire Police

Can you provide an overview of your role and experience in dealing with cybercrime in the context of small and medium enterprises?

I am the Cyber Protect Officer for the Hertfordshire Constabulary. My remit is delivering awareness, education and prevention advice to businesses and charities of all sizes and sectors and local communities, to help reduce the impact of cybercrime against the public and businesses.

Cyber security breaches and attacks remain a common threat to businesses of all sizes. However, worryingly, smaller organisations are identifying them less than last year (31% in 2023, vs 59% in 2022). This may reflect that senior managers in smaller organisations view cyber security as less of a priority in the current economic climate than in previous years, so are undertaking less monitoring and logging of breaches or attacks (source: UK Cyber Breaches 2023 Survey by the UK Government). Understandably, SMEs will view rising costs and more difficulty with financial planning, due to inflation, higher energy prices and the uncertainty about the economic situation as 'tangible' business risks, priorities and challenges.

There's a common misconception that cyber-attacks are only a "big business" problem and it's easy to see why. Cyber-attacks on larger businesses tend to grab the attention of the press because they involve familiar brand names and involve substantial amounts of customer data. But thousands of smaller businesses suffer cyber incidents each year.

What are some common cybersecurity challenges faced by SMEs?

In smaller organisations, the individuals responsible for cyber security tend to be senior management who already have many competing priorities in a challenging business climate and as a consequence, are not able to allocate adequate resources to cyber security.

In fact, the majority of all cyber-attacks are directed at small and medium-sized businesses. Small businesses are low-hanging fruit: Cyber criminals look for the easiest and fastest way to be successful. Smaller organisations may have less resources and time to train staff on cybersecurity risks, which makes them more susceptible to attacks like social engineering. They are also more likely to pay ransom demands when they feel like they don't have anyone to turn to for help.

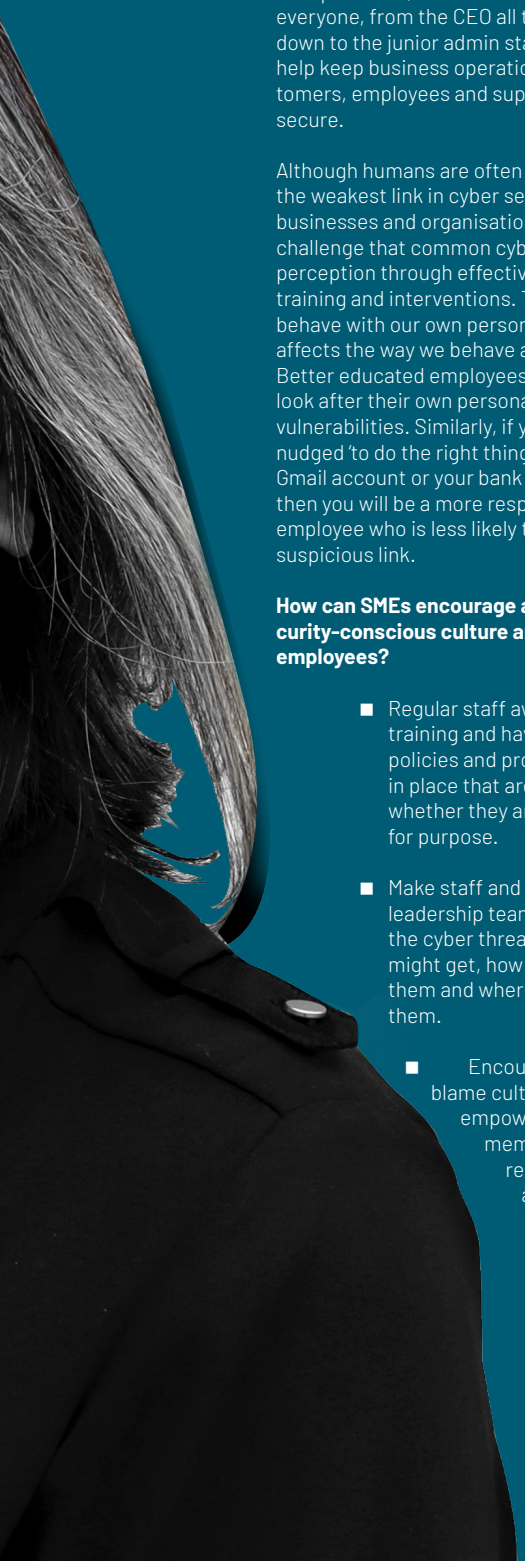
How do these challenges differ from those encountered by larger organisations?

Smaller organisations have the greatest tendency to use external contractors. There is a heavy reliance on IT providers and cloud storage providers when it comes to cyber security in general, as cyber security is still perceived as an 'IT problem'. Organisations most likely turn to these providers for advice and guidance following an incident. In a way, this delegated responsibility for cyber security may impact on the reduced need to come up with any internal processes and staff awareness training.

Suppliers can pose various risks to an organisation's cyber security - for example:

- third-party access to an organisation's systems.
- suppliers storing the personal data or intellectual property of a client organisation.
- phishing attacks, viruses or other malware originating from suppliers.

Few SMEs take steps to review the risks posed by their suppliers. Lack of time or money or being unable to get the information from suppliers and the lack of knowledge, are all barriers to businesses from undertaking a formal review of supply chain risks.



How important is cybersecurity awareness training for SME employees? Why?

There is a growing recognition that it is staff behaviour that drives most of the cyber security risk. The World Economic Forum says that 95% of cyber security breaches in organisations occur due to human error. We also know that 90% of organisations have not provided staff with cyber security training. These findings really highlight the importance of staff awareness and the critical role everyone plays in recognising this type of attack. Cyber security is not just the domain of the IT department, it is an issue involving everyone, from the CEO all the way down to the junior admin staffer, to help keep business operations, customers, employees and supply chains secure.

Although humans are often seen as the weakest link in cyber security, businesses and organisations can challenge that common cyber security perception through effective staff training and interventions. The way we behave with our own personal tech affects the way we behave at work. Better educated employees, frankly, look after their own personal tech vulnerabilities. Similarly, if you are nudged 'to do the right thing' in your Gmail account or your bank account, then you will be a more responsible employee who is less likely to click on a suspicious link.

How can SMEs encourage a cybersecurity-conscious culture among their employees?

- Regular staff awareness training and have relevant policies and procedures in place that are reviewed whether they are still fit for purpose.
- Make staff and senior leadership team aware of the cyber threats that they might get, how to handle them and where to report them.
- Encourage a no-blame culture, which empowers staff members to report their accidental cyber actions in a timely manner.

In short: cyber threats affect everyone in the business and everyone has a role to play in keeping its assets, data, reputation and people safe.

What are some cost-effective cybersecurity measures that SMEs can implement?

Cyber threats are amongst the most difficult to guard against. However there are some key considerations for companies.

- Have clear HR policies around staff leaving the organisation and ensure that they are adhered to. All staff leaving will have to document and audit exit interviews to include return of company IT equipment, password cancellations, etc. to limit opportunities for former staff members to be able to access company networks.
- Make staff aware of the approaches that they might get and how to report them. Discuss the actual examples as to keep the cyber threats alive in people's minds.
- Implement strong access controls and allow access to systems that people really need rather than everything. If you were working in a physical location, you might have some areas which were only accessible to staff who worked there and for anything valuable, maybe a safe. But you wouldn't give the safe keys to everyone who worked for you.
- Have internal network logging. This will enable you to see unusual activity, such as emailing eight thousand sensitive files outside of the network.
- Have policies and procedures which cover data control and access. Consider limiting the number of attachments that could be sent out at once and then set up a rule which alerts you if any more than that are sent. This gives you the ability to check that what is being sent is going for a legitimate reason. Tell your staff that their emails are being monitored and tell them about the policy.

What are some emerging cyber threats or trends that SMEs should be prepared for in the near future and where are these threats coming from?

The most common cyber threats are relatively unsophisticated. Businesses should protect themselves using a set of "cyber hygiene" measures including updated malware protection, cloud back-ups, passwords, restricted admin rights and network firewalls. As the most common attack vector remains 'phishing' – staff receiving fraudulent emails or being directed to fraudulent websites. This is followed by the impersonation of organisations in emails or online and viruses or other malware.

2023 is a pivotal year for the adoption of AI. AI-based tools attract criminals and less tech-savvy ne'er-do-wells to target victims for financial gain. We have already seen phishing by email, phone or online, becoming increasingly more sophisticated and targeted, with the deployment of readily available AI-based technology to craft sophisticated messages and to generate deepfakes – video, speech or images content of something that didn't actually occur – making it challenging to distinguish between real and fake content.

Cybercriminals and other bad actors often misuse deepfake technology. Some use cases include political misinformation, adult content featuring celebrities or non-consenting individuals, market manipulation and impersonation for monetary gain. These negative impacts underscore the need for effective deepfake detection methods.

How can SMEs stay updated and informed about evolving cyber risks and the latest preventive measures? Is AI an additional threat?

It goes without saying that technology is taking over the world and AI is a big part of it. As businesses are realising the power of AI and leveraging it because it makes work easier, boosts productivity and helps enhance client and customer experience and satisfaction - so do criminals. Criminals will find further ways to enhance their criminal capabilities using the tools we invent. While organisations can create chatbots, virtual assistants, recommendation engines, image and speech recognition software and predictive analytics tools with ethical safeguards, it isn't a difficult feat to re-implement the same technology without those safeguards. Criminals will not stop innovating - it has become even more essential to finding these fast-moving threats before a phishing email can turn into ransomware or data exfiltration. SMEs can get updates and follow news, trends and threats from government organisations, including the NCSC in the UK and major vendors in the field of cyber security solutions.