It’s time to turn rising cybe

The cyber-threat landscape never stays the same. With technology evolving at record rates and hybrid working creating more gateways for would-be attackers, the channel and its customers are under constant threat.

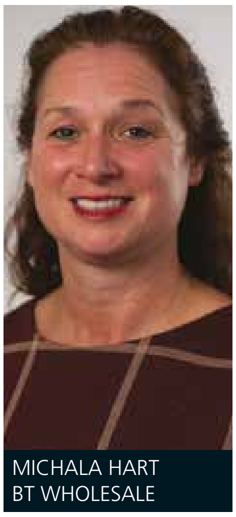
Working from home has increased the likelihood of cyber-attacks. A recent study by TextAnywhere, investigating the screen habits of 1,000 employees in the UK, revealed that 67.4 per cent are using their mobiles for work, imposing a serious threat to business security.

Resellers must make customers aware of the emerging technologies which have created a host of new risks to businesses. For example, there is great uncertainty about how IoT will affect the industry, with more dispersed endpoints creating a higher volume of vulnerable points. The GDPR PrivSec Report found that 47 per cent of the most vulnerable devices are security cameras installed on home networks, followed by smart hubs like Google Home and Amazon Alexa and network-attached storage devices.

For this month’s Kaleidoscope, we therefore asked industry experts a simple question: How can resellers safeguard customers against increasingly sophisticated threats and retain their position as a trusted and dependable business partner?

TIM SCOTT
ADEPT

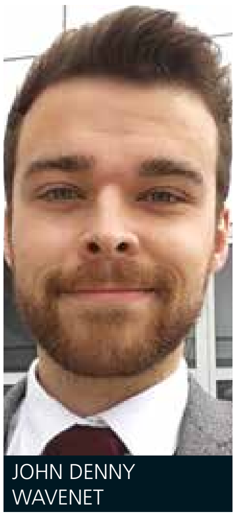
“Organisations operate in an environment no longer constrained by traditional physical boundaries, but one of highly distributed people, applications and data. This increases risk, which contributes to the growth in cyber threats and the industry’s adoption of the zero-trust concept of never trust, always verify. MSPs play a key role in educating customers on the modern threat landscape and the need for visibility and control across all aspects of their environment. A constructive approach is the Secure Access Service Edge (SASE) architecture. This provides a holistic access and security model and enables a good conversation about the broad range of risks, from different locations, and how they can be addressed. By approaching the discussion in this way, with a complete approach rather than point products and services, the MSP can act as a trusted advisor and consult on how solutions that address modern threats encapsulate how organisations work in a changing landscape.”


MICHALA HART
BT WHOLESALE

“Having good foundational cyber hygiene is by far the best way resellers can safeguard customers against the rapidly evolving threat landscape. Most breaches are a result of poor basic cyber hygiene either within the systems of the organisation, which are compromised, or within their supply chain network and digital ecosystem. If resellers focus on the basics and ensure that their own network and systems are patched and proactively monitored, they reduce the attack surface for themselves and their customers. Extending this advice and best practice to customers will earn trust and confidence. A good way to do this would be collectively adopting industry best practices such as the NCSC ten steps to cyber security which provides clear guidance to UK businesses. To further quote the NCSC, “cyber security is a team sport” we are safer together and proactively engaging will build long term trusted partnerships.”

LORRIN WHITE
BAMBOO

“Credibility and capability are top of the list when retaining customer trust. The best way of illustrating this in the rapidly expanding digital landscape is by showing you have your own house in order when it comes to mitigating and managing the heightened risk. Resellers should be able to confidently talk about the safety and security of their own ICT infrastructure and how they continually assess the attack surface of their business as it grows. If done right and resellers are demonstrably embedding digital assurance into every digital touchpoint then customers can take comfort that third party expansion simply knits into embedded processes and behaviours. If you really get it right, you ensure that your customers are additionally safeguarded by educating them throughout any technology change process too. To that end, it is equally important to understand and work through the infosec requirements of specific verticals and customers.”

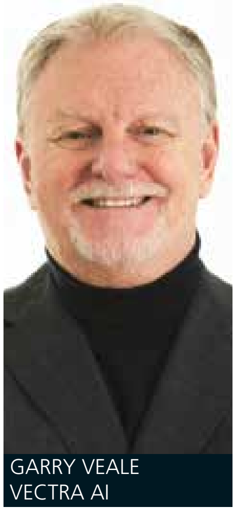

JOHN DENNY
WAVENET

“Our industry has always been one with an ever-changing landscape, and with this comes not only a great opportunity but also a great threat. New technology creates new avenues for customers to be compromised by those that would seek to cripple businesses for their financial gain. We have a duty as comms providers to stay on the pulse of these evolving threats, something that must be taken seriously. Delivering timely solutions that are proven to work, by partnering with the right solution providers, is the only way to ensure customers remain consistently protected. There is a responsibility therefore to vet these providers properly, not only from a technological perspective but from a cultural one too. Only those with the customer at heart will deliver, and continue to deliver, products and services that will protect customers for years to come, regardless of location: supporting hybrid, remote and office-based workers.”

RUSSELL HENDERSON
TRUSTACK

“In truth, it is not possible to completely safeguard a client against increasingly sophisticated cyber-attacks. The best you can do is to stay abreast of security best practices, evaluate, adopt and provide layers of protection using best-of-breed products to protect your clients. The onus also sits with the client to heed advice and invest in quality layers of protection. It isn’t a case of ‘it won’t happen to us’, it’s a case of when it does, how quickly can you contain the threat and limit the damage of either data encryption, data exfiltration, full-service outage, and reputational damage. Quality perimeter protection, solid endpoint protection, data loss prevention policies, data encryption, very robust backups, and cloud-integrated threat protection services are all necessary layers in today’s world to help reduce the possibility of an attack and limit the impact if one occurs.”

r threats into opportunities



GARRY VEALE
VECTRA AI

"As trusted advisors, it is up to partners to educate customers about increasingly sophisticated threats. The attack surface has widened, the traditional security perimeter has disappeared, and visibility is clouded. So, partners must advise customers to shift their mindset away from prevention-first strategies, which leave organisations blind to sophisticated attackers who are slipping through the net. This means adding technologies like AI and proactive threat detection solutions that can identify suspicious behaviours, so it is easier to stop attackers in their tracks. For example, technologies like Network Detection and Response and cloud-based security for services like Office 365 can increase visibility and enable organisations to stop attacks before they do any real damage. By convincing customers to take proactive security measures, they will have a better chance of avoiding breaches and being kept out the headlines."

ADRIAN SUNDERLAND
JOLA

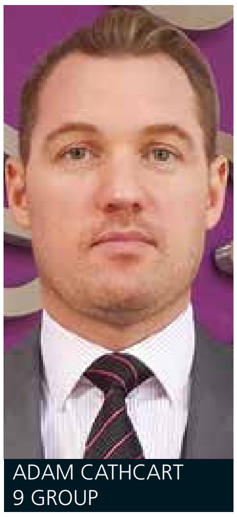
"There have been some high-profile cybersecurity attacks on IoT and M2M devices and deployments. Bristol Airport's flight information system was held for ransom and the digital signage in Union Street station was hacked so that information screens displayed hardcore pornography. There are also hidden attacks where IoT devices are used as botnets to power DDOS attacks, with device owners unaware until their monthly bill arrives. Jola is acutely aware of the need to protect our resellers and their customers from cybersecurity attacks. Our Mobile Manager portal, with its real-time alerting and control, provides visibility into the SIM usage before the monthly bill arrives. However, our approach goes beyond just managing the costs. If your application doesn't need internet access, then why would you expose it to the Internet? Jola offers SIMs that provide secure private access back to a corporate network without having any access to the Internet, eliminating the 'attack surface' completely."

ROAN PRATT
ENREACH

"Enreach has designed a cutting-edge cybersecurity strategy and defence system to ensure customers are protected against threats. As a telecommunication provider, we understand the importance of cybersecurity. The rate of change to all our systems can change in hours. As an organisation, we are constantly working to ensure that we are secured against growing threats to our customers. The benefit for our customers is having one platform and various product offerings that allow us to pivot quickly. Everyone at Enreach, from our customer service representatives to expert IT technicians, and everyone in between, understands the importance of security. We recognise that every SME has unique security needs, therefore we tailor our solutions to ensure that they are secured from any threats. We are dedicated to offering the finest results for every SME business. We address any cybersecurity difficulties for our customers and assist them to enhance performance."

GAIL LESLIE
KUBENET

"The Internet of things (IoT) is a great asset to our daily lives; and offers increasing potential to both how we build our businesses, and how we can interact with our customers. However, as the use of IoT rises, so too does the threat of a cyber-attack. As a trusted telecommunications provider, offering cyber security services, it is imperative to emphasise how measures such as firewalls and guest Wi-Fis (that can be set for just IoT use) enable protection to businesses, but it is also important to offer guidance into how to use IoT devices to their full potential. By introducing education and guidance, a trusting relationship is formed - helping position your business as an expert in this sector of technology and communications."



ADAM CATHCART
9 GROUP

"The pandemic resulted in a global shift towards hybrid working, creating opportunities for hackers to exploit new weaknesses. Attacks are becoming more sophisticated, as criminals constantly find new ways to outsmart existing technology. Responsibility for security doesn't just sit with business owners, it's firmly with the individuals within an organisation. However, Partners can add value by providing regular support and advice to customers, supporting them to reduce their vulnerability. Make security a focal point of your messaging and demonstrate that you are keeping pace with emerging threats. Holiday periods are particularly vulnerable times for telecoms fraud. Partners can take a proactive approach by contacting their customers to remind them of the risks and to provide guidance around the steps they can take to protect their business. We've worked closely with industry bodies to publish a fraud prevention checklist, for partners to share, enabling them to provide value to their own customers.

STEVE HENNESSY
BABBLE CLOUD

"The main strategy of resellers should be providing education on potential cybersecurity risks, whilst also ensuring protection is provided for their networks. As most attacks are due to end user error, it is vital to advise on additional security steps, such as multi-factor authentication, to minimise risks. To remain as a trusted and dependable business partner and provide organisational resilience to customers, reseller strategies should also incorporate: audit and education, focused on giving the customer control and knowledge of its network; recommendations, reviewing the network vulnerability with the customer and providing helpful questions such as, who has control over the security of your network? How quickly could you recover from an IT failure? Are all your IT systems and services documented?); finally, regular reviews should keep the customer informed on user training, network infrastructure and hardware etc."