PRESS RELEASE

Cyber-risks associated with new technology to become mainstream in 2020, according to Infosecurity Europe's CISO community

Security leaders predict next year's top trends, challenges and risks – technical debt, credential stuffing and access control are highlighted

Richmond, Surrey, UK, 0900 hours, 12th December 2019 – As we prepare to enter the third decade of the 21st century, Infosecurity Europe, Europe's number one information security event, has once again asked its community of C-level security professionals what they think the year ahead has in store. The list includes a range of challenges, opportunities, and broader trends across technology, business and the world.

Many of the CISOs highlighted the risks presented by **emerging technologies** that are expected to become more widely adopted in 2020. **Deloitte cyber risk partner, Peter Gooch**, says: "2020 will see more deployment of security automation tools. Where this is done well, it will allow organisations to adapt rapidly to changing attack tactics. Where it is done poorly, it will be more complicated to unpick.

"There will be a drive for more transparency when contracting for cloud services, with vendors required to expose more data and events for consumption by SIEM tools, and to evidence security practices and capabilities closer to real-time. Hackers are increasingly targeting unstructured data to hide and launch attacks, so the priority is to implement robust governance.

"More than 100 companies worldwide will begin testing private 5G by the end of 2020, which could increase the attack surface, making data flows harder to follow and the job of those responsible for securing them more challenging."

Mark D. Nicholls, Head of Information Security & Governance at housing association, Peabody, flags up vulnerabilities with AI and IoT. "Machine learning has established itself in 2019, and we will begin to move to true AI in 2020, but one must remember whatever can be used for good can also be used by the criminals. Imagine a DDOS attack powered by true AI," he warns.

"As consumers strive for a smarter, more connected world we will see more attacks targeting connected devices as a means to an end. This is not new, but the attack surface will get bigger. We must continue to educate to ensure humans are our strongest line of defence."

The **attack vectors** most likely to take centre stage in 2020 was another common theme. **Becky Pinkard, CISO at award-winning bank, Aldermore**, expects to see more attacks due to technical debt. "In the bid to keep pace with consumer demand and technology capabilities, industry is borrowing more technical debt than it's repaying. I think we'll see more headlines about successful attacks due to this growing debt and the associated 'shadow risk' it creates. The march to open banking in financial services, incorporating APIs, distributed ledger technology and AI in rapid-fire succession, and with a focus on capturing

the customer's attention first, often means security gets de-prioritised on the route to delivery."

"We're seeing credential stuffing run rampant, and I wonder if this will escalate as more data and more username and password pairs are out there," says **Troy Hunt, Microsoft Regional Director and Founder of Have I Been Pwned and 2019 and recent Infosecurity Europe Hall of Fame inductee.** "Or we might reach a tipping point where organisations decide they need to block some login attempts that have the right username and the right password but are not coming from the right person. In the US, enforcement cases are being brought against 'corporate victims' of credential stuffing. It'll either get worse, or organisations will have to adapt."

When it comes to the **security approaches** that will mitigate the risks which dominate in 2020, **David Boda, Head of Information Security, Camelot Group** believes 'back to basics' is best. "A focus on robust and timely access control and patching will still give the biggest reduction in risk for the majority of organisations across all sectors. These are the two areas that vendors, consultants and end user organisations should all be talking about."

Killian Faughnan, Group CISO of William Hill agrees that access control will be important – particularly in the next-generation workplace. "Access control is difficult to solve without being either too restrictive or too lenient. Given that in 2020, 35% of our workforce will be millennials, we need to find the right balance to enable employees in a way that works for them."

Some CISOs believe that solutions will come from the **industry working more closely together**. "I believe we will start to see greater collaboration between security companies, hopefully resulting in greater end to end security capability," says Mark Nicholls.

On a similar tack, Peter Gooch thinks convergence will be a key trend: "2020 could see a number of high-profile mergers and acquisitions as well an expansion and formalisation of vendors into a more converged world. This is likely to be similar to the ERP revolution that transformed the way many finance and operations teams function and could mean a more efficient operational model for those in cyber."

Two topics that were 'hot' in 2018/2019 are not front of mind with our CISOs this year. One of these is the **skills shortage**. "We will continue to talk about it," says Killian Faughnan, "though I think we may have hit a critical point, and that more companies will begin to recruit from pools of potential security professionals rather than existing ones. It's easier to teach a developer how to be an application security professional than the other way around."

There was also less focus on **GDPR**, probably due to the fact that the regulation and its impact are no longer the unknown they once were. **Paul Watts, CISO, Dominos Pizza UK and Ireland,** has observed signs of 'breach apathy' and wonders whether 2020 will see a continuation of this trend. "While this could be attributed in part to political distractions, I do think industry seems to be reporting more, but are the public caring less? I'm still reflecting on whether this is a blessing or a curse for CISOs as we move into the next decade…"

One question that is often pondered at this time of year is whether we're about to see **the 'mega breach'** that will put high profile incidents like Equifax's in the shade. "One thing we can never know is: will there be a crazy data breach that turns the world on its head again?", asks **Troy Hunt**. "If we see another incident like Ashley Madison or Equifax, which had a massive and serious impact across tens of millions of people's lives, this will be a headline-grabber that sticks around for some time. But these things are enormously hard to predict."

Nicole Mills, Senior Exhibition Director at Infosecurity Group says: "2020 will see the continuation of some long-standing trends, challenges and security risks. For example, a number of technologies that have been talked about for some time will become more widely adopted, and we need to be ready to implement, use and protect these in an appropriate way.

"There was less emphasis on the skills shortage and GDPR in our CISOs' predictions this year, but we do need to remember that these challenges haven't gone away. The 'talent gap' is still growing, and we need to continue working together as an industry to find solutions. And while GDPR is not the burning issue it was last year, organisations can't rest on their laurels. If they're compliant they need to work to stay compliant. It's not just the fines, keep top of mind that brand and reputation that can take years to redress."

Infosecurity Europe, now in its 25th year, takes place at Olympia, Hammersmith, London, from 2-4 June 2020. It attracts over 19,500 unique information security professionals attending from every segment of the industry, as well as 400+ exhibitors showcasing their products and services, industry analysts, worldwide press and policy experts. More than 200 industry speakers are lined up to take part in the free-to-attend conference, seminar and workshop programme. Find out more at https://www.infosecurityeurope.com

Ends

About Infosecurity Europe

Strategically held annually in London, Europe's centre for technology start-up businesses, Infosecurity Europe is Europe's largest and most comprehensive Information Security event. Featuring numerous analysts, policy experts, journalists and over 400 exhibitors, Infosecurity Europe presents an invaluable business platform, as well as staging the world's largest complimentary conference programme containing 240+ free to attend conference sessions which have been accredited by leading industry associations (ISC)² and ISACA since 2012. The event attracts over 19,500 unique information security industry professionals attending from every segment of the industry and presents the most important date in the calendar for information security professionals across Europe. www.infosecurityeurope.com. @Infosecurity #infosec20 #infosecis25

For further information, please contact:
Paula Averley, Origin Comms
t. 020 3814 2941/m. 07766 257776
e. infosec@origincomms.com