PRESS RELEASE

Threats and hacks were cybersecurity's greatest driving force over the last 25 years, say respondents to Infosecurity Europe poll

'Biggest ever data loss' will cause most damage in the next quarter-century

Improved technology will have twice as much impact on the industry's future as expanding the talent pool

Richmond, Surrey, UK, 0900 hours, X November 2019 – Evolving threats and hacks have had the biggest impact on moving the cybersecurity industry forward in the last 25 years, according to 39 percent of respondents to a social media poll conducted by Infosecurity Europe – Europe's number one information security event, which celebrates its 25th anniversary next year.

Necessity is the mother of invention. Constantly advancing technologies, attack vectors and techniques have forced the industry to keep innovating over the last quarter century. Necessary regulatory oversight and compliance requirements may also have kept CSOs awake at night, but only 17 percent of respondents believe these had a major influence on cybersecurity development. This could reflect a feeling that legislation and regulation have little real power to move the industry on – which might indicate a need to examine and update existing regulation, including the UK Computer Misuse Act which will be 30 years old in 2020.

The emergence of new technologies has helped the industry to make strides, according to respondents, with 25 percent agreeing that multi-factor authentication and (MFA) and encryption were catalysts for progress. Web security expert and creator of 'Have I Been Pwned?', Troy Hunt, agrees this has made a huge difference: "It's been recognised that a username and password are no longer enough, and now we have a range of different mechanisms from SMS to hard tokens. The adoption rates are still not particularly good, especially for external facing assets, but as a principle this is a fantastic thing – and where adoption is higher it does make a fundamental difference to the security landscape."

We're heading for a 'mega-breach'. Respondents to the Infosecurity Europe poll believe that the most damaging form of cyber-attack to happen over the next 25 years will be the world's biggest ever data loss (42 percent). This is followed by an attack on smart cities (30 percent), and an attack on critical national infrastructure (CNI) at 12 percent. Only 16 percent feel that the major event will involve ransomware – perhaps surprising given the considerable publicity given to this type of attack, and the high level of concern around it.

Nigel Stanley, Chief Technology Officer and global head of OT cybersecurity at TÜV Rheinland, says the likelihood of an attack on CNI should not be underestimated: "A systemic attack on a fundamental service or vital industry would cause widespread unrest, disruption and damage, and have a significant societal impact. But my concern are the attacks being carried out today. Vast amounts of intellectual property, knowledge and data

are being stolen as we speak and a future attack based on this could seriously challenge our defences, supporting systems and even way of life."

Better technology will improve cybersecurity more than solving the skills shortage, according to 38 per cent of respondents, followed by AI and machine learning (27 percent). Despite expanding the talent pool being a high priority across the industry, respondents believe this will only make a relatively small impact in the next 25 years (16 percent). This may be due to a lack of faith in the industry's ability to solve the key shortage, rather than a belief that doing so is of little importance. Again, regulation and compliance are not seen as a key driving force, with 19 percent saying that this will improve cybersecurity.

Nicole Mills at Infosecurity Group, says: "Threats and hacks have driven the evolution of the cybersecurity industry over the last 25 years, and they probably always will do. The major concern around the future is data-loss – it appears that data is still king, and this is expected to remain the primary motive for cyber-attacks. We should be thinking hard about where the next big attacks will be – the healthcare or finance sectors, for example – and whether we need to do more now to prevent them. It's good news for vendors that technology is perceived to hold the key to the future of cybersecurity, and they must keep on improving their products and services to meet this expectation.

"As individuals, as organisations and as an industry, we must all continue to work hard to stay one step ahead of the attackers. There will be plenty of opportunities at Infosecurity Europe 2020 for visitors to hone their skills and their strategies and explore cutting-edge innovations and companies. These include FutureSec, a series of events and sessions that address the future of the information security industry by focusing on people and innovation."

Attracting 8,290 responses, the Infosecurity Europe Twitter poll was conducted during the week of 4 November. Infosecurity Europe also asked its community of CISOs for their views on innovation in cybersecurity.

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