PRESS RELEASE

Attack on critical national infrastructure is imminent, say over half of respondents to Infosecurity Europe poll

Convergence between physical and cyber environments is leaving businesses exposed

Richmond, Surrey, UK, 0900 hours, 26 February 2019 – More than half (59 per cent) of respondents to the latest social media poll conducted by Infosecurity Europe 2019 – Europe's number one information security event – believe that an attack on the UK's critical national infrastructure is likely this year.

As more devices, systems and infrastructure are connected to the internet, the cyber and physical worlds are becoming increasingly linked, opening up new attack vectors. According to Ciaran Martin, head of the UK's National Cyber Security Centre (NCSC), a major category one (C1) attack on our critical infrastructure – one that disrupts essential services, or affects national security – is a matter of "when, not if".

The responses to Infosecurity Europe's poll also indicate that organisations in all sectors are not properly prepared to manage security effectively across both cyber and physical environments. Lack of collaboration and low levels of awareness of key legislation are the biggest problems. The challenges and complexities posed by the convergence of cyber and physical security will form a key part of the conference programme at this year's Infosecurity Europe 2019 event.

Over two thirds (68%) of respondents say the security teams in charge of their physical and cyber infrastructures never collaborate. This disconnect leads to misaligned plans and conflicting priorities, while creating 'silos' that make it difficult for CISOs to gain full visibility of controls and risks across both IT and OT (Operational Technology) environments.

"Defending critical assets is a team sport," says Nigel Stanley, Chief Technology Officer and global head of OT cybersecurity at TÜV Rheinland. "IT, physical and OT teams need to get their act together and start to share and learn from each other."

Kevin Fielder, Just Eat's Chief Information Security Officer, agrees. "The increasing convergence of cyber and physical environments is inevitable, but managing them in a cohesive way will strengthen enterprise security." According to Kevin, it's the insider threat that needs most urgent attention. "Those intent on accessing money, information or IP will often find it easier to do so from the inside – and we're moving to a world where this can mean immediate impact to life. Hacking a building's management systems, for example, could suppress a fire alarm or sprinkler system, or prevent people leaving."

Only 16 per cent of respondents to the Infosecurity Europe poll were aware of the EU's NIS Directive – which is designed to improve the security and resilience of network and information systems – and its implications. The legislation, which was put in place in 2016, sets out security requirements that apply to all operators of essential services and digital service providers (DSPs). Failure to adhere to these could leave security gaps that present attackers with ‘open doors’ through which they can access infrastructure and physical assets. UK organisations found to be non-compliant can be fined up to £17 million.

“I can’t believe that any cyber security leader in a sector impacted by the NIS Directive would be unaware of its implications for their business,” says Nigel Stanley. “Lack of commitment to secure critical infrastructure is the worst sort of negligence. Forget what the regulators demand – organisations should take the initiative and secure assets based on a proportionate cyber security and business-led risk assessment.”

Kevin Fielder believes that if the industry doesn’t take the lead, further regulation will follow. “It really is in our best interest to self-regulate and protect the public. If the industry doesn't produce connected devices that are, by default, secure and manageable over the long term, it won't take many real incidents for government regulations to quickly materialise.”

Victoria Windsor, Group Content Manager at Infosecurity Group, says: “The security challenges resulting from the convergence of physical and cyber environments will take centre stage at Infosecurity Europe 2019 – and for good reason. Operational systems in every industry are being connected to corporate and cloud environments, and the safe ‘air gap’ between IT and OT no longer exists. Cyber risk is now impacting the physical realm, and organisations must have effective management strategies in place. Technology such as unified threat management tools has a role to play, but it’s also vital that teams collaborate and communicate to understand blended cyber-physical attacks, and develop joint approaches, plans and policies.”

Attracting 12,100 responses, the Infosecurity Europe Twitter poll was conducted during the week of 4 February. Infosecurity Europe also asked its community of CISOs about the challenges presented by the increasing convergence of cyber and physical domains, and how security can be managed in a cohesive way.

Infosecurity Europe, now in its 24th year, takes place at Olympia, Hammersmith, London, from 4-6 June 2019. It attracts over 19,500 unique information security professionals attending from every segment of the industry, including 400+ exhibitors showcasing their products and services, industry analysts, worldwide press and policy experts, and over 200 industry speakers are lined up to take part in the free-to-attend conference, seminar and workshop programme - 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 #infosec

For further information, please contact:
Paula Averley, Origin Comms
t. 020 3814 2941/m. 07766 257776
e. infosec2019@origincomms.com