PRESS RELEASE

Human skill and expertise singled out as the most important element of a cyber resilience approach by over 40 per cent of respondents in latest Infosecurity Europe poll

Findings cast the spotlight on the growing pressures faced by information security workers and the need for more to be done to protect their mental health

Richmond, Surrey, UK, XX00 hours, 19 February 2020 – More than 40 per cent of respondents in the latest Twitter poll run by Infosecurity Europe, Europe's number one information security event, singled out human skill and expertise as the most important element of a successful cyber resilience approach. The aim of the poll was to explore the importance of resilience in cybersecurity; that is the ability of an organisation and its cybersecurity professionals to prepare, respond, and recover when cyber attacks happen.

With the number of cyber attacks faced by organisations growing on a daily basis and a projection that 146 billion records will have been exposed in the five-year period from 2018-2023, the pressure cybersecurity professionals are under has never been greater. Couple this with the threat of regulatory fines, reputational damage and the growing skills shortage - there are nearly 3 million unfilled cybersecurity positions at companies worldwide – it's clear that protecting individuals and enhancing their resilience should be a key priority for organisations.

Human skill and expertise was the clear leader with 40.5 per cent of respondents in answer to the question **what is the most important element of a successful cyber resilience approach?**, next was implementing best practice at 22.5 per cent, and 20.1 per cent said governance and compliance. Implementing advanced technology was considered their lowest priority at 16.8 per cent.

Paul McKay, Senior Analyst at Forrester Research, and a speaker at this year's Infosecurity Europe, is in agreement: "Undoubtedly human skill and expertise is the most important element of a cyber resilience approach. You can have all of the technology and best practice approaches deployed in the world, but ultimately successful cybersecurity relies on the skills, ingenuity and cognitive ability of the human brain. Many of my clients have gaps in their security team caused by difficulties in finding enough people to fill open roles on their teams. This impacts them critically both in progressing their security program, but more importantly, the mental, physical health and wellbeing of everyone else who are often doing heroic work making up for gaps in their teams. I don't think I've ever seen security professionals under this much pressure."

The poll examined the repercussions of the pressures faced by workers asking information security workers the question **have you ever made significant mistakes as a result of being overstretched or stressed at work?** Over half said yes; 26.8 per cent answered yes, significant errors, while a further 31.9 per cent said yes, minor mistakes had been made. A quarter (25 per cent) said no and 16.2 per cent didn't know. Unsurprisingly a recent report found that 65 per cent of IT and security professionals considered quitting due to burnout.

Becky Pinkard, Chief Information Security Officer with Aldermore, who will also be speaking at this year's event, said: "The average life-span for CISOs is quite frightening. One of the last stats I've read it's just 18-24 months. When you start to look at that and relate that back, literally anyone in cyber security will be able to tell you a time when they've made a mistake, whether that's because they didn't know what they were doing, were stressed out, or they felt under pressure from project management or timeline pressure, and we are constantly faced with the same constraints so it will always be an issue we need to recognise and deal with."

Maxine Holt, Research at Ovum shared her thoughts: "I haven't witnessed anything directly but have heard of plenty of instances of security incidents and breaches that are accidental (don't know doing wrong) or negligent (know circumventing procedures just to get the job done) in nature, and for sure some of these can be attributed to lack of time or stress. For example, having to follow a convoluted process to log a sale might be bypassed just because someone has a target that they must meet, it's the last day of the sales period, and a person's job depends upon it. There is plenty of anecdotal evidence in both the private and public sectors."

Employee mental health and wellbeing should be an essential consideration for all employers and none more so than those working in information security but is enough being done? Responses to the question **does your organisation provide mental health support to its employees who are responsible for dealing with a cybersecurity data breach or attack** were resounding with a staggering 45.5 per cent answering no, 31.6 per cent didn't know and just over a fifth (22.8 per cent) said yes they were being offered support.

Kevin Fielder, CISO at Just Eat believes organisations need to be doing more: "It's a high pressure, always on role that can easily burn people out. Organisations need to really recognise this and provide support for their teams. As a manager I also try to make the team and working environment as flexible and supportive as possible." **Kevin says the best kind of support is**: "An organisation that genuinely invests in it and makes support/counselling available to all plus a team culture that is supportive - I think the right team is absolutely critical to success here."

Independent Researcher, Dave Edwards says: "Security is a very stressful job, as risk decisions needs to be made. Good decisions are not always a popular choice, they can delay projects and cost revenue. Companies can do more, I have had a positive experience, although this is about company culture and organisational values; senior leaders such as CIOs, Directors, etc., need to lead and set an example though good behaviours as they cascade across an organisation for all staff."

Cyber resilience will form a core theme for the 2020 event and will be covered extensively as part of the Conference programme at Infosecurity Europe 2020 (2-4 June, Olympia, London) which is now open for registration, visit here for more information.

Nicole Mills, Senior Exhibition Director at Infosecurity Group says: "We as Infosec professionals and leaders need to be resilient ourselves – developing new skills and on a personal level, being resilient to the stress and pressure facing people in our industry.

"Our poll clearly highlights that human skill and expertise is the most important aspect in building a strong cyber resilience strategy and this is why organisations need to focus on providing a safe and supportive environment to protect their most important asset. By building the expertise of those involved at the sharp end of cyber attacks and taking measures to provide them with mental health support will not only help to strengthen resilience, but it will attract and reassure those wanting to enter the industry."

Drawing 6,686 responses, the Infosecurity Europe Twitter poll was conducted during the week of 10 February. Infosecurity Europe also asked its community of CISOs and analysts for their views on resilience in cybersecurity.

Infosecurity Europe, now in its 25th year, takes place at Olympia, Hammersmith, London, from 2-4 June 2020. It attracts over 14,000 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