PRESS RELEASE

Almost half of respondents to latest Infosecurity Europe poll "wouldn't know" if their organisation had suffered a cyber breach

Findings highlight significant 'holes' in incident response capabilities – particularly around post-breach communications and visibility of information assets

Richmond, Surrey, UK, 0900 hours, 22nd January 2020 – Almost half of respondents to the latest Twitter poll run by Infosecurity Europe, Europe's number one information security event, admit they would be completely unaware if a cyber breach occurred in their organisation. The poll was designed to explore incident response, an area that has come under recent scrutiny following Travelex's response to its New Year's Eve cyber-attack, which left many of its systems down and impacted travel currency sales.

In answer to the question ***"If a cyber breach occurred, how quickly could you discover it?"*** 31.5% of respondents said they would discover it immediately, 14.3% within 30 days, and 6.6% within 200 days. However, a shocking 47.6% conceded they simply wouldn't know.

According to **Maxine Holt, Research Director at Ovum**, this reflects a widespread issue. "Discovering a breach well after the event is usual. Uncovering breaches is not easy, but proactive threat hunting is an approach being increasingly used by organisations. Regularly scanning environments to look for anomalies and unexpected activity is useful, but it can be difficult to deal with the number of resulting alerts. Ultimately, effective cyber hygiene involves having layers of security to prevent, detect and respond to incidents and breaches."

Good incident response demands good risk insight. The poll examined this by asking ***"What understanding do you have of your information assets?"*** A worrying 44.7% revealed they had "very little" understanding, with 30.7% stating they had "some" – and only 24.7% said their grasp was "comprehensive".

Bev Allen, Head of Information Security Assurance, CISO, Quilter, says: "Many companies don't know what or where all their information assets are. They may think they do; but if they're wrong this leaves them vulnerable to breaches. Consistent knowledge of your assets takes effort; you need tools and systems to record what you have, you need people to follow appropriate processes, and you need to search to find out what you don't know about and where it is. This search must be done regularly."

Steve Trippier, CISO of Anglian Water, believes the 'knowledge gap' is due to a lack of awareness of the need for effective asset management. "It often falls behind other

processes in terms of priorities, as its value can be less immediately obvious. As more companies introduce automated vulnerability discovery and management, the need for effective asset management will become very obvious, especially as cyber teams highlight vulnerabilities on assets that the organisation forgot it even had!"

The poll also uncovered potential evidence of skewed priorities around post-breach actions. Travelex released a series of statements after its December attack, but received criticism from customers for a lack of information about when service would return to normal, and whether sensitive customer data had been accessed, as the gang behind the attack claimed.

In response to the question ***"What is the key priority when dealing with the fall out of a major cyber-attack?"***, getting back to business topped the list for 42.4% of respondents, followed by customer communications and PR (23.6%), engaging law enforcement (19.4%) and ensuring compliance (14.6%). This indicates that more time and energy might need to be refocused on the communication side of incident response.

"PR can make or break a breach," agrees **Maxine Holt**. "Arguably British Airways did a decent job, whereas Equifax did not. Ultimately, the 6-Ps mantra should be at the forefront of organisations' minds: proper preparation and planning prevents poor performance. Being ready for a cyber-attack, security incident or data breach in general means that the organisation has a much better chance of emerging out of it in a reasonable state."

Becky Pinkard, Chief Information Security Officer with Aldermore also highlights the need for proper planning. "Good incident response requires attention across all areas – from public relations management to deep technical expertise, and everything in between. However, companies largely fail due to two reasons: they lack any documented incident response plan, and if they do have a plan they've not 'stress tested' it."

Incident response is set to be a key cybersecurity theme for 2020 and will be covered extensively as part of the programme at Infosecurity 2020 (2-4 June, Olympia, London).

Nicole Mills, Senior Exhibition Director at Infosecurity Group says: "Working to prevent breaches will always be imperative, but the cybersecurity industry is increasingly recognising that this is not always possible, and that how organisations respond to and recover from a breach is incredibly important. The results of our poll indicate that improvements need to be made in areas including breach detection, the thorough preparation and rehearsal of response plans, and the discovery and classification of information assets.

"They also highlight that while having a clear strategy to restore 'business as usual' as quickly as possible, immediate and transparent communication with customers – and also

partners, suppliers, and regulators – is necessary to preserve trust and protect the brand's reputation. This means PR departments should be part of the incident response team."

Attracting 6,568 responses, the Infosecurity Europe Twitter poll was conducted during the week of 13 January. Infosecurity Europe also asked its community of CISOs and analysts for their views on incident response 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. Celebrating its 25th edition this year, 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