UK Sees Wave Of Cyber Breach Reports After GDPR

Law360, London (September 12, 2018, 5:02 PM BST) -- The U.K.'s data regulator is receiving around 500 calls a week to its hotline for reporting information breaches, nearly four months after Europe's data protection regime went live in May, a senior official said Wednesday.

Around a third of calls come from organizations who speak with the Information Commissioner's Office before deciding that the breach does not meet the General Data Protection Regulation's reporting threshold, James Dipple-Johnstone, the ICO's deputy commissioner, said.

"The ICO does not seek perfection even if to some it may feel like that," Dipple-Johnstone told delegates at a cybersecurity conference in London. "We seek evidence of senior management and board level insight and accountability."

Banks and insurers faced a last-minute rush to prepare for the GDPR, which exposes firms to mammoth fines for data breaches, before it entered into force on May 25. In Britain, lawmakers have carved out a generous exemption that will let the insurance industry keep processing medical and criminal record data as usual.

Today, one in five breaches reported to the ICO involve cyber incidents, of which nearly half concern phishing, or fraudulent attempts to trick customers into sharing sensitive information. Of the remainder, 10 percent involved malware and six percent concerned malware attacks, he said.

Organizations are struggling to understand the GDPR's requirement to report a breach within 72 hours and some of their reports to the data regulator are still incomplete.

"Remember it's not 72 working hours, the clock starts ticking from the moment you become aware of the breach," he said. "You might not have all that information to hand in the first 72 hours, we get that, but please plan ahead." Firms should have people with suitable seniority and clearance to talk to us and be ready to provide as much detail as they can, he added.

“It is not very helpful to be told there is a breach affecting lots of customers but the reporter isn’t authorized by the general counsel to tell us more than that!” he said.

Dipple-Johnstone also warned that some data controllers are over reporting and said it would work with organizations to try and prevent this.

“If you adopt privacy by design, treat cybersecurity as a boardroom issue, and demonstrate a robust culture with appropriate transparency, control and accountability for your and your customers' data, then we will not usually have an issue with you should the worst happen,” he said.

The GDPR carries fines of £17 million ($22 million), or four percent of global turnover, whichever is higher. Firms must give customers the right to have their data deleted and must report a cyberattack within 72 hours.