Global Counsel

Will the EU's new cybersecurity law prevent another Yahoo?

Blog post by Adviser Conan D'Arcy, 23 September 2016

The data security world has been rocked by Yahoo's revelation that it had been the victim of a "state sponsored" hack leading to the exposure of 500 million user accounts. Beyond the sheer scale of the breach, its significance lies in the apparent lack of transparency with users, who were only notified this week when the incident is reported to have occurred in 2014. This opacity does not appear limited to Yahoo's customers since even Verizon, which is acquiring Yahoo for $4.8 billion, has issued a public statement clarifying that it had only received "limited information and understanding of the impact".

Yahoo is far from the first company to disclose data breaches after the fact - US healthcare insurer Excellus BlueCross disclosed in August 2015 that it been suffered a breach dating back to 2013. These examples have heightened concerns that the incentives for companies facing cyber-attacks are aligned against transparency, particularly where this incurs immediate financial and reputational risk. The experience of British telco TalkTalk has served as a salutary lesson on the risks of transparency for many corporates. Having disclosed a major data breach speedily and publicly, the company faced months of negative media coverage, the loss of over 100,000 customers and, in the immediate aftermath, a major decline in its share price. Complacency on cybersecurity has manifested itself in a lack of preparedness within companies with the Institute of Directors (2016) finding that 80% of British companies had no cyberinsurance, 51% had no internal training and 43% had no cybersecurity strategy.

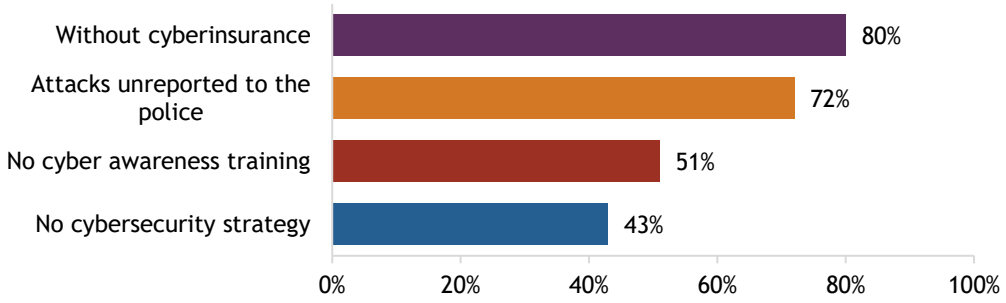

Fig. Lack of cyber security strategies and procedures
Source: IoD Cyber Survey 2016

There is evidence that the public are becoming increasingly concerned about the security of their data and there is a danger that delayed disclosures could further undermine trust in online security. Evidence from Eurobarometer polling shows that 54% of the EU's public have major concerns about disclosing their personal data online. Policymakers have, however, been slow to catch up and, despite critical statements today from regulators, such as the UK's Information

Commissioner's Office, there has been resistance from national governments in Europe to be more proactive in compelling companies to disclose data breaches to regulators and the public.

The EU's Directive on Security of Network and Information Systems (NIS) goes some way to addressing the gaps in the regulatory system. "Critical infrastructure" such as banks, energy utilities and airlines will have to report cyber breaches to national regulatory authorities and introduce internal processes for managing and responding to such attacks. Under certain circumstances, national regulators could choose to notify the public of such breaches. However, ambition for a more comprehensive cybersecurity approach, covering a broad sweep of online platforms in its scope, was frustrated by EU national governments, including the UK, who shared the concerns of companies that a proactive approach on cyber transparency could present significant commercial risks.

The result has been that the NIS directive is unlikely to prevent a repeat of the Yahoo data disclosure. The new rules will not come into force until mid-2018 and, when they do, email platforms such as Yahoo will not be captured by its disclosure rules and, even if they were, they would not necessarily compel Yahoo to publicly disclose the breach. In the longer term, policymakers may have their hands forced if the Yahoo incident is repeated by other major companies. This may lead to a scenario where the EU institutions find themselves legislating on new, broader and tougher rules before the NIS directive has even had time to bed in, a phenomenon seen during the financial crisis when there were examples of EU financial services rules undergoing revision before the implementation of the predecessor round of reform.