17 Dec 2015

businessinsider Daily Record

Comment: EU to introduce mandatory cyber security reporting

16:50, 17 DEC 2015 | BY DAILYRECORD.CO.UK

Lindsay Urquhart, associate with bto solicitors' Data Protection Defence Team

Lindsay Urquhart, associate with bto solicitors' Data Protection Defence Team

Europe's Cyber Security Directive, which aims to strengthen European resilience to cyber-attacks, will have substantial implications for key infrastructure providers such as communications, cloud computing, some e-commerce platforms, healthcare, energy, banking and transport operators.

The Directive is intended to improve the ability of member states to co-operate and respond to cyber threats.

The Directive will introduce mandatory reporting of security breaches for key infrastructure providers in energy, transport, financial markets, health and water.

Once the Directive has been approved in Europe member states will have 21 months to implement the Directive in National Law and a further six months to identify "operators of essential services".

These operators will be subject to enhanced security requirements and will be subject to the mandatory reporting requirement.

Member states will be required to introduce Computer Security Incident Response Teams (CSIRTs) who will work co-operatively with the EU Agency for Network and Information Security (ENISA) to improve cross border incident handling and response.

Presently, ENISA is reporting that security incidents and human error in these key infrastructures result in annual losses in the range of €260- €340 billion Euros, and that currently there is no co-ordinated approach to security and reporting within the EU

The text of the Directive still needs to be formally approved by member states, the presidency will present it for approval by member states' ambassadors at the Permanent Representatives Committee on 18 December 2015.

Formal adoption by both the Council and the Parliament is required before the Directive will become law in Europe.

The changes are, however, likely to lead to greater continuity in respect of security standards which will benefit those providers with operations in multiple European jurisdictions. Commentators are calling for a light touch from regulators, particularly, given the wide scope of services including information and communication technology services that may be covered by the Directive.

Although the immediate effects of increased security requirements will be felt most keenly by large infrastructure service providers, we anticipate a knock on effect as these larger operators look to secure their supply chains by imposing increased security requirements in contracts and procurement processes.