Essential services companies that fail to comply with the NIS Directive could face fines of £17 million

ELY, CAMBRIDGESHIRE, UNITED KINGDOM, August 10, 2017 /EINPresswire.com/ -- IT Governance, the leading provider of information security and data protection expertise, is urging organisations that operate in the essential services sector to start complying with the Network and Information Security (NIS) Directive.

This comes in response to consultation plans announced by UK Digital Minister Matt Hancock, which outline requirements and obligations in line with the NIS Directive and aim to help essential services businesses and infrastructure across the EU prepare for continually evolving risks and cyber threats.

Alan Calder, founder and chief executive officer of IT Governance, said: “The consultation announced today confirms that the UK government has committed to implementing the NIS Directive and therefore organisations operating within these critical sectors will be required to adopt risk management practices and report major incidents in line with the requirements of the Directive.”

The NIS Directive provides EU member states with legal measures to increase the level of cyber security, which will be adopted in UK legislation by May 2018, despite Brexit. It requires organisations within member states to implement these measures and build a security culture across all sectors vital to society and the economy.

The Directive sets out significant security obligations for organisations that supply essential services and operate in critical sectors such as energy, transport, banking, health or digital services.

Matt Hancock said: “We want the UK to be the safest place in the world to live and be online, with our essential services and infrastructure prepared for the increasing risk of cyber attack and more resilient against other threats such as power failures and environmental hazards.”

The Directive introduces penalties that will be based on member countries’ discretion, with the UK government warning of fines of up to £17 million or 4% of global annual revenue for organisations that fail to protect themselves from cyber attacks. Digital Service Providers (DSPs) and Operational Executive Services (OESs) organisations will face additional penalties to those raised by data breaches under the General Data Protection Regulation (GDPR).

Organisations that are required to achieve compliance with the NIS Directive should urgently look into ways of reducing their cyber risks and implement incident reporting and business continuity management programmes.

IT Governance recommends that businesses start by achieving compliance with the international best-practice information security standard ISO 27001, combined with the international business continuity standard ISO 22301.

To find out how IT Governance can help organisations comply with the NIS Directive by implementing a cyber resilient management system based on ISO 27001 and ISO 22301, please visit our website, email servicecentre@itgovernance.co.uk or call +44 (0)845 070 1750.

- Ends -

NOTES TO EDITORS

IT Governance Ltd is the single-source provider of books, tools, training and consultancy for IT governance, risk management and compliance. It is a leading authority on data security and IT governance for business and the public sector. IT Governance is 'non-geek', approaching IT issues from a non-technology background and talking to management in its own language. Its customer base spans Europe, the Americas, the Middle East and Asia. More information is available at www.itgovernance.co.uk.

Mihaela Jucan
Miss
+441353771078
email us here
