The intersection between regulation and cyber security is becoming more overt, warns IT Governance

Following the launch of the UK government's Cyber Essentials Scheme: Requirements, it appears that businesses will soon face another compliance challenge

ELY, CAMBRIDGESHIRE, UK, May 7, 2014 /EINPresswire.com/ -- Following the recent launch of the UK government's Cyber Essentials Scheme: Requirements, it appears that British businesses will soon be facing another compliance challenge. The Assurance Framework linked to the scheme is expected to be launched later this year and will allow independent certification against the scheme.

Despite not being a law, established international information security frameworks such as ISO27001 and PCI DSS are widely seen as minimum contractual requirements. With a growing number of new laws and regulations, how can organisations ensure they address the ever-increasing compliance challenges around digital security and data protection imposed by their governments?

Alan Calder, Founder and Executive Chairman of IT Governance, says: "The intersection between regulation and cyber security is becoming more overt. If you look at the various laws and regulations worldwide, you will recognise that cyber security underpins most of them in one way or another. For example, the Data Protection Act in the UK, the Protection of Personal Information Act (POPI) in South Africa, the Health Insurance Portability and Accountability Act in the US and other state level breach laws, have all been enacted to protect personal data.

"Adopting a joined-up approach to compliance and cyber security will become increasingly important for organisations. It will enable them to protect their information assets while complying with various legislative and regulatory requirements more efficiently."

Cyber security is driven by a number of factors, including governmental security concerns, customer and stakeholder pressure, corporate competitiveness and survival.

Calder continues: "The approach to compliance and the approach to cyber security are very similar – in both cases an organisation needs to take process, people and technology into account, while ensuring that the confidentiality, integrity and availability (CIA) of information is kept intact. The CIA model is at the basis of every information security management system, but it's also very relevant to compliance."

Implementing a cyber security framework based on best practice will help organisations create a systematic approach to compliance.

Calder advises that organisations build internal knowledge of the international ISO27001 cyber security standard which is going to play an ever more important role in meeting their compliance objectives. He is the author of the books An Introduction to Information Security and ISO27001:2013 – A Pocket Guide and The Case for ISO27001:2013, which are available from the IT Governance website: www.itgovernance.co.uk/shop/c-117-books.aspx.

Desislava Aleksandrova
IT Governance Ltd
00448450701750
email us here