Critical infrastructure organisations need a cyber resilience strategy

/EINPresswire.com/ Critical infrastructure companies have long been target of cyberattackers, especially advanced persistent threats (APTs), with the objective of stealing information or compromising information systems. In addition to the cyberattacks critical infrastructure companies can be affected by weather changes and other unforeseen circumstances which can lead to severe disruptions in operations. Experts warn that having a cyber-resilience strategy in place is of paramount importance to critical infrastructure companies for ensuring operational continuity.

Alan Calder, CEO of cybersecurity experts IT Governance, says, “Cyber-resilience means that an organisation's systems and processes are resilient against outside attack or natural disaster. This is best achieved by integrating an organisation’s information security management system (ISMS) with its business continuity management system (BCMS).

“Severe weather leading to power cuts and traffic disruptions can affect organisations really badly. It can be particularly damaging for critical infrastructure companies, on which all of us are reliant. Unless they have well managed business continuity system to ensure continuity of operations the situation can easily get out of control.”

Calder adds, “The importance of mitigating the disruption to information technology services has been at the heart of disaster recovery and business continuity plans for many years. Ensuring that an organisation’s IT systems and processes are resilient against natural disaster or outside attack is a key principle underlining the ISO22301 and ISO27001 standard.”

Organisations can integrate the two systems by using the ISO/IEC 27031 Guidelines for ICT Readiness for Business Continuity. ISO/IEC 27031 provides a bridge between general business continuity management and information technology tying together ISO/IEC 27001 and ISO22301 to information and communications technology (ICT) business continuity preparedness.

Critical infrastructure companies can obtain internal knowledge and skills of implementing and integrating both systems by sending staff to specialist training. Both ISO27001 Certified ISMS training courses and ISO22301 Certified BCMS training courses are available from IT Governance. They can be booked online at www.itgovernance.co.uk/training.aspx.

- Ends -

FOR FURTHER INFORMATION
Desi Aleksandrova Marketing Executive
+44 (0) 845 070 1750
daleksandrova@itgovernance.co.uk

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.
