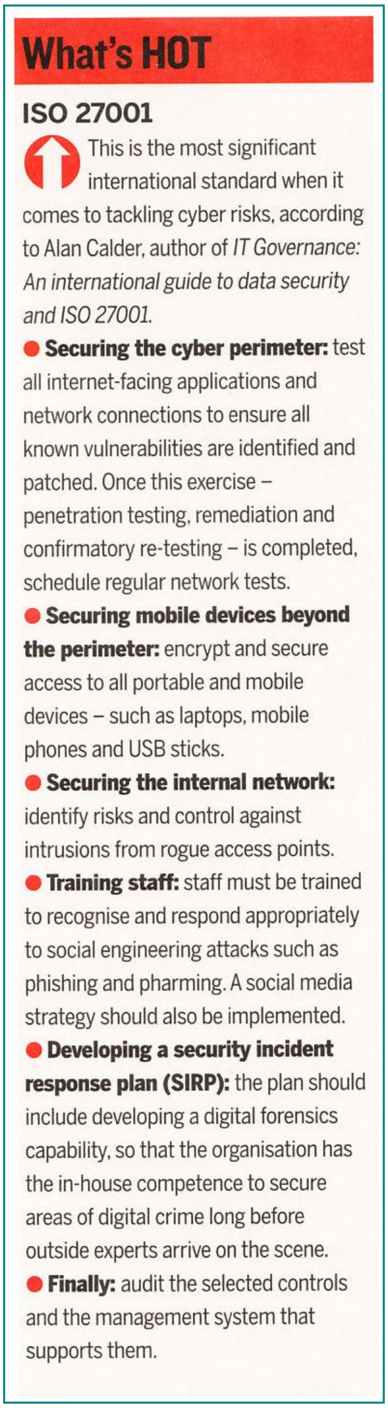
SC Magazine

July-August 2012



What's HOT

ISO 27001

This is the most significant international standard when it comes to tackling cyber risks, according to Alan Calder, author of *IT Governance: An international guide to data security and ISO 27001.*

- **Securing the cyber perimeter:** test all internet-facing applications and network connections to ensure all known vulnerabilities are identified and patched. Once this exercise – penetration testing, remediation and confirmatory re-testing – is completed, schedule regular network tests.
- **Securing mobile devices beyond the perimeter:** encrypt and secure access to all portable and mobile devices – such as laptops, mobile phones and USB sticks.
- **Securing the internal network:** identify risks and control against intrusions from rogue access points.
- **Training staff:** staff must be trained to recognise and respond appropriately to social engineering attacks such as phishing and pharming. A social media strategy should also be implemented.
- **Developing a security incident response plan (SIRP):** the plan should include developing a digital forensics capability, so that the organisation has the in-house competence to secure areas of digital crime long before outside experts arrive on the scene.
- **Finally:** audit the selected controls and the management system that supports them.