CYBER RESILIENCE - THE NEW NORMAL

A GUIDE TO IMPLEMENTING A SUCCESSFUL CYBER RESILIENCE STRATEGY

Everything you need from a single source:

www.itgovernance.co.uk/cyber-resilience-critical-issues.aspx

Protect • Comply • Thrive

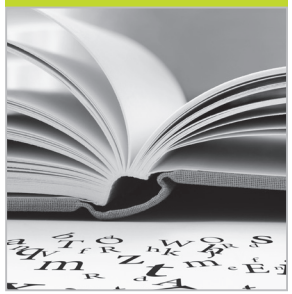
1. SECURE THE CYBER PERIMETER

Test all your Internet-facing applications and network connections to ensure that all known vulnerabilities are identified and patched. This should include testing all wireless networks. Make sure that OWASP and SANS Top 10 vulnerabilities and security weaknesses are patched.

The solution - click on the images below for more information

Cyber Resilience Standards

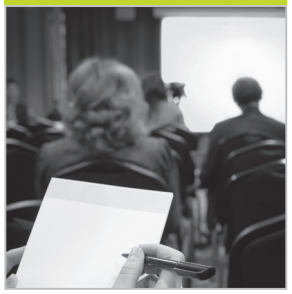
Books On Penetration Testing



Penetration Testing As A Service

Risk Assessment With vsRisk™

Managing Cyber Security Risk Training



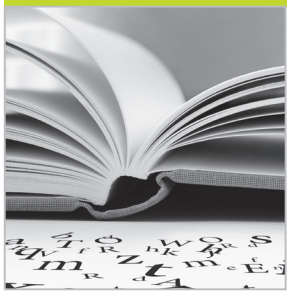
Cyber Resilience Suite

2. SECURE MOBILE DEVICES BEYOND THE PERIMETER

Encrypt and secure access to all portable and mobile devices (laptops, mobile phones, BlackBerrys, USB sticks, etc.) to ensure that the increasingly elastic network perimeter remains secure and that data taken beyond the perimeter remains secure.

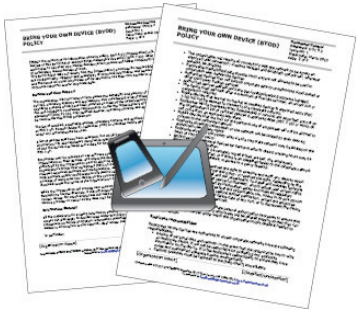
The solution - click on the images below for more information

Books About Encryption



BYOD Documents And Policies

Device Encryption



BYOD (Bring Your Own Device) Policy Template Toolkit
Fully up to date with ISO27001:2013, this BYOD (Bring Your Own Device) toolkit offers organisations the prospect of more efficient working and a better work-life balance for employees.

3. SECURE THE INWARD- AND OUTWARD-BOUND COMMUNICATION CHANNELS

This encompasses channels such as e-mail, instant messaging, Live Chat, and so on. Make sure there are appropriate arrangements for data archiving and an appropriate balance between protecting confidentiality, integrity and availability.

The solution - click on the images below for more information

Information Classification Tools

Boldon James information classification software allows you to apply relevant classifications (visual and metadata labels/protective markings) to information (files) of many different types. These labels/markings can be used to enforce user policies, raise user awareness of security and orchestrate multiple on-demand security technologies such as encryption.

boldonjames
A QinetiQ Company

4. SECURE THE INTERNAL NETWORK

Identify risks and control against intrusions from rogue wireless access points, unauthorised USB sticks and mobile data storage devices (including mobile phones, iPods and so on).

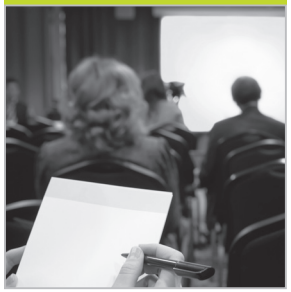
The solution - click on the images below for more information

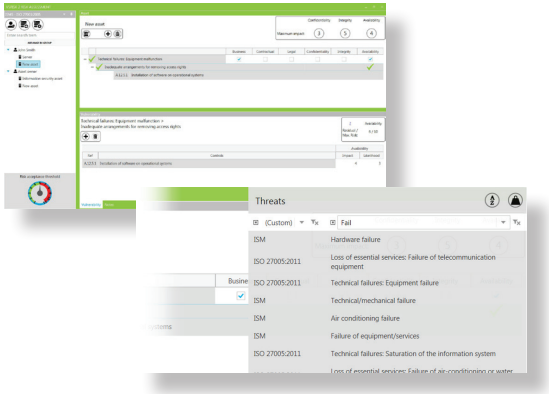
Cyber Resilience Health-Check

Penetration Testing As A Service

Risk Assessment With vsRisk™

Managing Cyber Security Risk Training





vsRisk

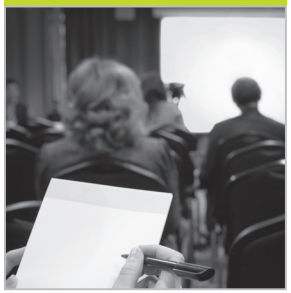
Automated Information Security Risk Assessment

5. TRAIN YOUR STAFF

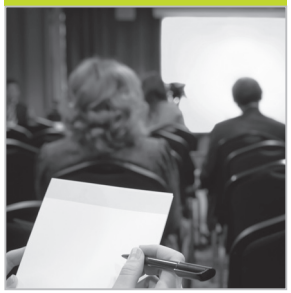
Attackers understand that employees are the weakest link in the security chain, and take advantage of natural human weaknesses through a style of attack known as social engineering. Staff must be trained to recognise and respond appropriately to social engineering attacks that range from tailgating to phishing, spear phishing and pharming.

The solution - click on the images below for more information

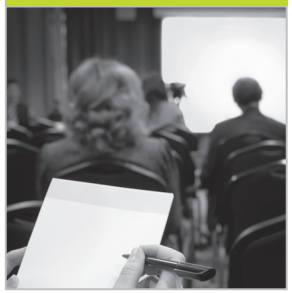
ISO27001 Training



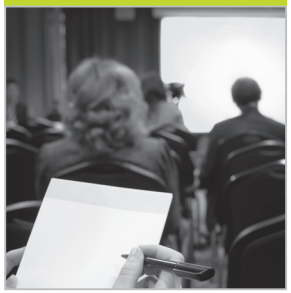
ISO22301 Training



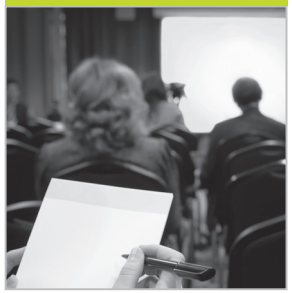
Managing Cyber Security Risk Training



CISSP Training



CISM Training



Staff Awareness E-learning

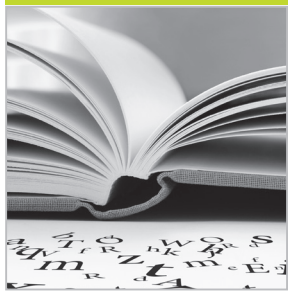
6. DEVELOP AND TEST A SECURITY INCIDENT RESPONSE PLAN (SIRP)

Sooner or later your defences will be breached, and you need an effective, robust plan for responding to that breach. Your response plan should include developing a digital forensics capability so that you have the in-house competence to secure areas of digital crime long before outside experts arrive on the scene.

The solution - click on the images below for more information

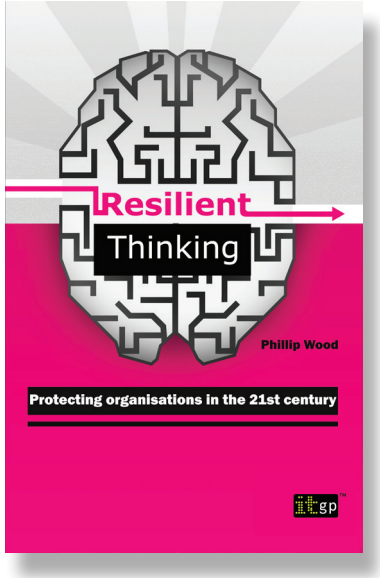
Incident Response Standards

Books On Resilience



Cyber Resilience Suite

Business Continutiy Impact Analysis



7. ADOPT APPROPRIATE INFORMATION AND CYBER SECURITY STANDARDS

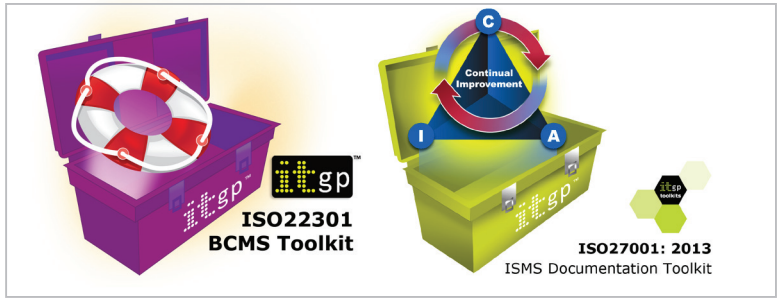
The adoption of key standards not only assures you of your organisation's security and response capability, but certification assures business partners and customers that their information is safe in your hands. Standards provide the guidance and accumulated wisdom of years of best practice, and help ensure the protection of your information.

The solution - click on the images below for more information

Cyber Resilience Standards

Incident Response Standards

Cyber Resilience Suite



Cyber Resilience Implementation Suite
Everything you need to set up a cyber resilient management system.

CONTACT US

w: www.itgovernance.co.uk

t: + 44 (0) 845 070 1750

e: servicecentre@itgovernance.co.uk

@ITGovernance

/it-governance

/ITGovernanceLtd

Books

Toolkits

Training

E-learning

Software

Consultancy