Cyber Security Health Check

With cybercrime now bigger than all other types of organised crime put together, it's essential that you regularly assess and monitor your business risk against a cyber attack.

We work together with cyber security experts to help identify the weaknesses within your organisation and implement processes and controls to reduce cyber threats and eliminate vulnerabilities.

Our Cyber Security Health Check will look at all aspects of your business, sensitive, critical information and data, and identify those areas at risk, requiring improvement and urgently needing action. Our industry-leading team will then provide a full detailed report complete with recommendations and next steps.

Businesses of all sizes are at risk; no business is too small, no sector is safe - you may think so, but the cyber criminal will and does think otherwise.

Our Services

- Information and cyber security health check report and next step recommendations
- Managed service of information, security management and cyber security
- Virtual information security manager or virtual CISO (chief information security officer)
- Full internal audit against your own policies and procedures or in preparation for Cyber Essentials Scheme or International standards
- Development or guidance on building your information and cyber security documentation. Policies and Procedures, including Information (security) risk, business continuity, incident and disaster recovery
- Development or guidance to meet International standards specifications or UK National standards Cyber Essentials and Cyber Essentials Plus ISO/IEC 27001
- Information and cyber security accredited training and cyber awareness
- Managed service for data privacy (DPA2018, GDPR and related regulations.

Cyber Security

Penetration Testing:

- External, internal testing and website
- Web and mobile apps
- Wireless, VPN assessments, Social engineering, physical access
- Red team and scenario-based assessments
- Incident response and disaster recovery
- Cyber security training and development of awareness campaigns.

Information Security

ISO/IEC27001:2013 (and sector-based codes of practice, including Cloud services)

- Information (security) risk management (ISO 31000:2018 and ISO/IEC 27005:2018)
- Documentation – policies, procedures, guidelines
- Internal Audit.

ISO/IEC 27701:2019 (privacy information management extensions to ISO/IEC 27001:2013 and ISO/IEC 27002:2013)

- Incident response – planning and preparation; and operations
- Business Continuity – ISO 22301
- Information security management training.

Data Protection

Data Protection Act 2018 (including GDPR)

- Assessments (e.g. data privacy impact assessments) and data flow mapping
- Internal audit
- Employee training and development of awareness campaigns.

Your Key Contact -

Barry Maxey
Director of Client Technology

T: 01228 690114 | M: 07469850632

barry.maxey@armstrongwatson.co.uk