Risk Management: Cyber Security Resources

The following is a list of useful organisations and websites that may assist you in managing cyber security.

Data Protection

Protecting personal data in online services: learning from the mistakes of others

This is a publication by the Information Commissioner's Office (ICO). It discusses eight areas of computer security that have frequently arisen during investigations of data breaches by the ICO. These are: software updates; SQL injection; unnecessary services; decommissioning of software or services; password storage; configuration of SSL and TLS; inappropriate locations for processing data; and default credentials.

ICO - Protecting personal data in online services

Data Protection Self-assessment Toolkit

Use the toolkit to assess your compliance with the Data Protection Act and find out what you need to do.

Data Protection Self-assessment Toolkit

Encryption to Protect Data

Information Commissioner's Office guidance

This provides a link to the ICO website guidance on encryption.

ICO - Encryption

Information Sharing About Threats

Cybersecurity Information Sharing Partnership (CiSP)

The Cybersecurity Information Sharing Partnership (CiSP), part of CERT-UK[1] , is a joint industry government initiative to share cyber threat and vulnerability information. CiSP allows members from across sectors and organisations to exchange cyber threat information in real time in a secure and confidential environment. CiSP members are also able to receive network monitoring reports. This free service allows users to receive tailored feeds of information from CERT-UK covering any malicious activity seen on your network.

CiSP

IT Security

Information Commissioner's Office guidance

This is aimed at small businesses and gives advice on how to keep IT systems safe and secure.

A Practical Guide to IT Security

Miscellaneous

Ten Steps to Cybersecurity

This guidance is for businesses looking to protect themselves in cyberspace.

Ten-step Summary - Cyber-Risk Management

Standards in Cybersecurity

Cyber essentials scheme

The Cyber Essentials scheme is a government-backed, industry supported scheme to help organisations protect themselves against common cyberattacks. The Cyber Essentials scheme provides businesses, small and large, with clarity on good basic cybersecurity practice. By focusing on basic cyber hygiene, your company will be better protected from the most common cyber threats. It enables organisations to gain one of two Cyber Essentials badges.

Cyber Essentials Scheme

ISO/IEC 27001: Information Security Management

The Information Security Management system is a systematic approach to managing sensitive company information so that it remains secure. It includes people, processes and IT systems by applying a risk management process. Certification to ISO/IEC 27001 is possible, but is not obligatory.

ISO 27001 Information Security Management

Training in Cyber Security

Cybersecurity for Legal and Accountancy Professionals

This is a free course, which has been developed by the UK government as part of its National Cybersecurity Strategy, with the support of both the Law Society and the Institute of Chartered Accountants in England and Wales (ICAEW).

Cybersecurity Training for Legal and Accountancy Professionals

[1]**CERT-UK** is the UK National Computer Emergency Response Team, formed in March 2014 in response to the National Cyber Security Strategy.

The National Cyber Security Strategy, published in 2011, sets out the importance of strengthening the UK's response to cyber incidents.