Quiss

Excellence through experience

The level of protection should reflect the value of the asset

The growing sophistication of cyber-attacks means there is an inevitability of a security breach for most organisations, risking loss and reputational damage.

The key to protecting assets is first to recognise what is valuable, then to assess what level of protection is appropriate. You cannot protect everything all of the time – the more valuable the asset, the greater protection required. We have created a three-step solution to help organisations prepare for the increasing threat of cyber-crime and the likelihood of an attack.

Blended Learning Consortium

Exclusive Blended Learning Consortium Offer

QUISS TECHNOLOGY PLC

Claymore, Tame Valley Industrial Estate, Tamworth, B77 5DQ

TELEPHONE 0333 222 4334 EMAIL enquiries@quiss.co.uk www.quiss.co.uk

Quiss

Excellence through experience

Our three-step solution to help organisations prepare for the increasing threat of cyber-crime and the likelihood of an attack.

Step one

The Data Protection Act requires you to use appropriate technical and organisational measures to ensure data is safe and secure.

It doesn't prescribe what safe and secure means, but the least that might be expected would be an asset register, so you know what information you have, where it is and who has access to it.

Through a FREE initial consultation, we will get to understand a little more about your establishment which will highlight any weaknesses both in terms of security and Data Protection Compliance. Combined with a free training session for senior decision makers within your establishment this will enable you to decide how to best protect your assets from a security breach.

A combination of people, policy, process and technical measures will deliver the right level of protection for the various assets within your organisation.

Step two

Having evaluated your assets and established the physical environment and human factors at play, the next step is to look carefully at your IT infrastructure, systems, electronic communications and business continuity options.

We interrogate your current security arrangements to ensure systems are protected from unauthorised access, including network monitoring, access management, encryption levels and a review of your protection against viruses, malware, phishing attacks etc.

The review leaves nothing to chance, as the use of cloud services and in particular cloud data services increases the challenge of protecting your data in all the various locations you keep it and require access to, often remotely.

And it's not just your internal processes and systems that are examined, we also assess the security requirements of your relationship with third-party suppliers and clients who may have access to your valuable assets.

Step three

We are all human and it is a fact of life that no matter how well prepared we are, accidents do happen.

A free, no obligation review will explore the various options in cover available that are most appropriate for your business in respect of Cyber & Data Insurance.

This FREE review can also extend to a full review of your insurance programme, ensuring it is correctly aligned to your business activities and assets so that your cover responds at the time when you most need it.

Solutions from a wide range of insurers will be considered to ensure the most appropriate solution is always recommended.

If there is nothing to rectify in either steps one or two, we will still share our reports and offer some valuable suggestions for the future. But when we find potential risks or the cost of protecting less valuable assets is too high, we will explain in detail what is required to ensure you reduce your chances of becoming another victim and tomorrow's headline.

It might be policies and processes or the start of your journey to ISO 27001 certification. You might require new hardware, a more robust infrastructure or a more closely monitored network, but whatever you need, Quiss can help.

This offer is available only to members of the Blended Learning Consortium and resources are limited, so please get in touch today and secure your FREE asset and security assessment.

Blended Learning Consortium

Exclusive Blended Learning Consortium Offer

QUISS TECHNOLOGY PLC

Claymore, Tame Valley Industrial Estate, Tamworth, B77 5DQ

TELEPHONE 0333 222 4334 EMAIL enquiries@quiss.co.uk www.quiss.co.uk