



daisy.

SECURITY
CONSULTANCY



Cyber Security

ASSESS AND IMPROVE YOUR CYBER SECURITY POSTURE

Understanding the cyber threats facing your organisation and the measures you currently use to protect against them are vital in stopping cyber attacks. The cyber security landscape is continuously changing, so keeping up to date with the latest technology and recommendations can be almost impossible without outside assistance.

Daisy's security consultants are available to help you either as a one-off engagement or as a trusted extension to your IT team working with you on an ongoing basis. Our experienced consultants can help you get your security strategy working effectively from helping you understand your biggest risks, recommending improvements to helping you attain cyber certification and writing effective security policies.

Security Health Assessment

The Security Health Assessment provides an external review of your 'cyber security maturity based on good practice and informed by frameworks such as Cyber Essentials and the Centre for Internet Security (CIS)'s 'Top 20 Critical Security Controls'.

A Security Health Assessment by Daisy's skilled security consultants can review the controls you have in place and make targeted recommendations to help improve your security posture. The assessment can also be used to measure progress over time or provide evidence of an investment requirement.

What does the Security Health Assessment deliver?

The scope of the Security Health Assessment covers cyber security people, processes and technologies, including:

- Executive/senior management sponsorship
- Governance, policies and processes
- Threat prevention technologies
- Deployed and configured technology and services
- Detection and response capability

Did you know?

Daisy's security experts can also help with writing security policies, including incident response plans, attaining compliance such as PCI DSS and Cyber Essentials, and designing, deploying and managing complex security infrastructure.



SECURITY
CONSULTANCY

As part of the assessment, Daisy's security consultant will:

- Review relevant documentation, including processes, policies and infrastructure topologies
- Host a meeting to gather as much information as possible about the organisation's risk profile and deployed cyber security technologies
- If possible, hold a short call with a member of the board of directors/executives
- Create a report outlining findings from each topic with associated recommendations and score
- Present the report back to your organisation

Virtual Security Manager

A chief information security officer (CISO) or security manager is responsible for developing and implementing an organisation's information security policies, processes and protections. However, many organisations do not have a large enough IT team to dedicate a single individual to lead this ongoing necessity. Whilst someone can perform the role part-time, they will often lack the training and experience in developing a robust security posture. They may be ineffective at reducing vulnerabilities and reducing your exposure to risk.

The Virtual Security Manager service provides specific security expertise to your IT team. Our advisors will work on your behalf to improve your security posture and protect against cyber security attacks.

What does the Virtual Security Manager deliver?

While the Virtual Security Manager service is bespoke to each organisation, the common tasks include:

- Develop and implement a threat management strategy with input from critical areas of the organisation
- Advise on the selection, design and deployment of security products and services
- Plan security assessments and reviews, help interpret the results and create resolution plans
- Help the organisation move towards achieving compliance with relevant industry standards such as GDPR and Cyber Essentials (Plus)
- Provide informal training to IT and security staff
- Provide oversight of breach response
- Review security information and event management (SIEM) platforms, investigate alerts and make mitigation recommendations
- Create and maintain security policies and incident response plans

Why Daisy?

Daisy has a 25-year track record of supplying managed security services:

- The best technology – highest levels of accreditation with the world's leading vendors
- Skills and expertise – state-of-the-art UK-based 24/7 Security Operations Centre (SOC)
- Certification - Daisy is certified to ISO 27001 for information security management, and our security advisors hold certificates including CISM, CISSP and CEH

Have you thought about...?



Cyber Security

Security Information & Event Management (SIEM) – to better understand your threat landscape and be able to react to threats in real-time



Professional Services

Customer Design Authority – for unbiased advice and recommendations to help you on your technology journey



Find out more about Daisy's Security Consultancy, speak to one of our sales specialists today:

enquiry@daisyuk.tech

0344 863 3000