



Security Posture Review – Data Sheet

Here at Voyager we have developed our own technology focused framework to assess the posture of your organisation from a holistic approach. Our framework is an amalgamation of the key areas from NCSC's '10 Steps to Cyber Security' and the 2018 Cyber Essentials blue print.

What is Security Posture?

The world of cybercrime is an ever growing and evolving industry worth billions. Along with this evolution, new vocabulary is developing in unison. A new addition is the concept of 'Security Posture', but what is it?

The security posture of an organisation refers to its overall security strength across multiple areas of the IT estate. Traditionally, security solutions have been fragmented with a large volume of organisations believing that a secure 'network' makes for good security posture. This is not true. To truly improve security posture and minimise your overall cyber risk, organisations of today must take a holistic approach by reviewing and securing the 8 key areas of security posture.

Why do I need to understand my Security Posture?

To make good decisions, you need good information. Our technology focused security posture review helps your organisation to understand its current posture by iterating its strong points, areas for improvement, and weak points – all alongside detailed recommendations. Armed with this information, your organisation can make well informed decisions to ensure your cyber risk is nominally low and that you are maximising the ROI from your existing investments.

Our Approach

We focus on 8 key areas of your organisation's IT to provide a truly holistic approach. We take into consideration bare metal network and security devices, wireless infrastructure, cloud services, web and email protections, remote working technologies and policies, end user policy & control, and more.

| | |
|---------------------------------------|--|
| Network Security | Networking and security devices Implementation best practices Security architecture and network topology Security of the data plane (wired and wireless) Ongoing security monitoring |
| Secure Configuration | Secure configuration of management planes Build processes Patching and vulnerability management Device hardening |
| Access Control | User access control to organisation resources and services Wireless access control Physical access to equipment IT employee screening Company leavers process & Contractor access |
| Malware Protection | Network and host based malware protection Installation policies & Update procedures |
| Web & Email Protection | Cloud email and web security On-premise email and web security Web & email DLP |
| Home & Mobile Working | Remote access technology BYOD policies & Teleworker policies |
| Removal Media Controls | Control over mass storage Mass storage malware protection Mass storage DLP |
| User Education & Awareness | Policies and procedures for new starters and ongoing training for existing staff Board level involvement Acceptable use policy |

About Voyager

Voyager Networks is an IT Solutions business delivering a range of innovative solutions to its many clients across a wide range of public and private organisations. Solutions can be provided on-premise, from a data centre or in a hybrid environment to best suit business needs. Additionally, working in partnership with a number of finance houses, we can provide both Capex and flexible Opex purchasing models.

In summary we make complex networking and communication technologies simple to deploy and support – **IT MADE SIMPLE.**