CYBER WARDEN

PRACTICAL CYBER RISK MANAGEMENT

Recently the UK National Cyber Security Centre (part of GCHQ) issued a threat report regarding targeted attacks against the UK legal sector (https://www.ncsc.gov.uk/files/Cyber-Threat-Report_UK-Legal-Sector.pdf).
This is an excellent report, and contains great advice on how to protect against such attacks. It's 24 pages long, and quite dry, but here's our take on it.

1) It's not just the UK legal sector being targeted – this is a global issue affecting other sectors including Accounting, Healthcare, Engineering, Construction, Hospitality, and Education.
2) The advice isn't anything new or specific to the legal sector.
3) Confidentiality (therefore trust) and money is at stake.

Summarized below is the advice from the report, and how we and our partners can help:

Attack	Control	How we can help
Phishing	Implement DMARC, SPF and DKIM	Included in all Mail Aegis service levels
	User Education	We can provide user awareness materials and training
	Use Anti-malware solutions	Mail Aegis Silver and Gold scans all inbound mail for malware. In addition, our IT partners can help you implement an effective XDR platform across your IT estate.
	Incident Reporting & Management Plan	We can help tailor all IT policies and plans. These are a major stepping stone to ISO/IEC 27001 compliance.
Business email Compromise (BEC)	Monitor for and remove impersonation domains	We can provide advice on how to secure and defend against likely impersonation domains
	Unusual request validation process	Included in the IT policies suite.
	Strong passwords & MFA	Audit and implement as per agreed IT policies.

Ransomware & Malware	Immutable offsite backups	Included in Mail Aegis Gold for M365 and Google Workspace. Also available separately for all services, including self-hosted data.
	Patch Management	Define in IT policies and enforce through technical controls and processes.
	Software Inventory & Management	Measure via Systems Management platforms with our IT Services Partners
	Strict Remote/Cloud Access Management	Define through policy, implement various access controls as appropriate, including MFA. This may also include time of day or physical location controls.
	Business Continuity Plan	Included in the IT Policies suite.
Password Attacks	Unique, strong passwords for each service	Define via policy, including using MFA and secure password management software.
	Least Privilege access	Define via policy, include AAA controls.
	No Account Sharing	Define via policy, disable all shared accounts and provide individual accounts for all staff and contractors. Auditable
	Change all default passwords	Define in IT policy & procedures, Auditable.
Supply Chain Attacks	Supply Chain Mapping	Work with you to identify the supply chain, identify risks, provide process to remediate or mitigate risk.
	Incorporate security into supplier contracts	We can work with you regarding the wording that should be included in supplier contracts and help to measure compliance via a variety of techniques.

The above looks pretty complicated, but it’s not really that difficult or expensive to implement, and can be done in stages at a pace that works for your business, and doesn’t cause operational issues for the business.

We would consider the above recommendations to be the absolute minimum steps that you should be implementing to help protect your business, but it’s a good starting point. Our policies and procedures will take you beyond the above recommendations.
For all businesses, the first step should always be an assessment, then start working on reducing risk as transparently as possible.
Typically, these will include:

- Implement Mail Aegis.
- Implement MFA across all platforms.
- Implement a Systems Management and XDR platform.
- Implement recommended policies and procedures.
- User Awareness/Training
- Supply Chain mapping & associated security audit/validation.

Our policy is to work with your existing IT team or IT services provider, and where there are gaps, make recommendations on how to fill them.

We don’t provide any public customer references, or publicly share which resellers we work with due to confidentiality and security reasons, however these can be provided on request and agreement of all concerned parties.

If you already work with an IT services supplier, we can work directly with them where they can resell our service, retaining simplicity for your business, both from a billing and support perspective.

Contact us at info@cyberwarden.io