Cyber Minimum Standards

As the Cyber insurance market continues to become more disciplined in its approach to underwriting, it's now more important than ever to prepare for increased underwriting scrutiny. Our recent experience suggests that the below minimum standards must be met in order for underwriters to be able to consider quoting for your cyber risk exposure:

- MFA (Multi - factor Authentication) across entire organisation as a general approach – it needs to be in place for all administration and privileged accounts, remote access, and email accounts. Privileged accounts need MFA even when those users are accessing accounts in the office, so it is not just limited to remote access.

  Further MFA may be required depending on the business and the insurer's stance.
- No use of End-of-Life systems, unless segregated from main network, offline, or behind firewall.
- Network segmentation if appropriate for type of organisation. Information Technology and Operational Technology estates to be segregated from each other.
- System segmentation – front-line and back-up systems segmented. The client will be expected to encrypt PII data and their back-up environment.
- BCP (Business Continuity Plan / Disaster Recovery Plan) in place and tested regularly (at least annually) including a test of back up procedures. It should include cyber attacks and events.
- Back-ups kept separate from main network (offline) or in cloud service designed for this purpose (insurers are looking for back-ups to be kept offline too as they have seen a number of cases where cloud back-ups were deleted or corrupted or affected by the original attack and have therefore been rendered unusable – this leads to greater costs for data restoration and business interruption).
- System back-up - Where the client has not tested the ability to successfully restore key data from back-up in the last 6 months.
- Firewall/network perimeter defences in place.
- Software patches to critical systems applied in short time frame (aim for 7 days, below 30 ideally is the maximum).
- Endpoint Protection (EPP) and Endpoint Detection and Response (EDR). For larger risks (£500m+ turnover), EDR will be expected.
- Regular employee training (including Phishing training) – to be carried out at least once a year.

- Annual penetration testing.
- Vendor Management – whilst this is not a minimum standard as such, insurers are seeking greater understanding on how firms are managing their exposures with their vendors, including the due diligence undertaken when onboarding a new vendor and throughout the working relationship.

Please note that the above does not necessarily reflect a "definitive" list – different insurers will apply different standards, and their expectations are continually evolving. Even if you meet with all of the points highlighted above, it is no guarantee that an insurer will quote your risk in current cyber insurance market conditions. However, we believe that applying the above standards will substantially improve your chances of obtaining competitive cyber terms.