The Corporate
IT Forum.

Ten Cyber Security Tips from CITF Members

1. The first stage must always be to evaluate data for suitability for being cloud based and to do a risk assessment. Only commit information to the cloud once you have completed that risk assessment on loss, corruption and non-availability.
2. Contracts with Cloud service providers are often one sided (in the CSP's favour) and members find they are very unlikely to get them changed. In reality, members make risk based decisions on the CSP's profile, track record and history of incidents.
3. Members generally use well known and established providers (Office 365, Salesforce, Azure for example). These products have a proven track record for security.
4. Data storage needs to be in compliance with EU legislation and safe harbour/privacy shield rules. The list of countries considered safe is likely to change under GDPR. Members can decide on where data (including back-up and DR) can reside if the data is hosted outside of the UK.
5. Members realise we need to deal with 'Shadow IT'. IT needs to embrace cloud solutions for faster availability. If IT doesn't the users will go it alone. Members are proactively connecting with the business to help them get their cloud solutions faster. But the members agree that we need to raise awareness of risks of Shadow IT.
6. Larger member organisations have established good governance frameworks to ensure a consistent and approved approach to managing and security cloud services covering set-up, approval of new suppliers and how to manage access to the portals.
7. It is important to establish a monitoring policy and produce supporting policies to continually monitor systems and networks. This should also include home and mobile working.
8. Threat reduction includes good authentication, most often a two stage process with a security token (dongle, ATM card, mobile phone etc).
9. End-users need to be educated in the risks of security. Bothe the access of on-line sites and the physical hardware. Organisations have a legal obligation to protect personal and sensitive data. An organisation can be fined if a member of staff leaves their unencrypted laptop on a train.
10. Members are aware that, although rare, they need to be able to retrieve their data in they want to change suppliers (or even rarer, that the supplier ceases to trade). This is often over-looked, but should be included in DR and business continuity planning.