Know the warning signs

The increasing number of digital initiatives such as Bring Your Own Device (BYOD), affecting the way organisations do business has led to an exponential growth in the threat of security breaches and cyber attacks. Additional risks branch from the increasing need of agile IT systems that enable faster collaboration, communication and immediate access to information, leading to the use of unsecured external IT platforms and the rise of Shadow IT.

The cost of cyber attacks– both financially and in reputational damage – can be huge. From loss of competitive advantage with customers taking their business elsewhere following a breach, to regulatory fines, to loss of business as a result of system downtime, it's clear that minimising the threat of cyber attacks must be a strategic priority for every organisation.

In this panorama, where cyber crime is more mature than ever and technology trends around sharing data evolve at a fast pace, knowing what signs to look for in order to avoid a security breach is vital for any business. The more you know about your security environment, the better you are able to protect your organisation and avoid potential security breaches.

Source: http://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-digital.pdf

The following questions highlight some of the most important areas where you might be vulnerable. If you answer "yes" to any of them, your organisation might be at risk.

Top **5** questions:

Do you support BYOD (bring your own device)?	no ☐	yes ☐
Does shadow IT (employees using non-corporate, preferred systems) exist?	no ☐	yes ☐
Are your security rules not rigorously enforced, or not implemented right through to C-level?	no ☐	yes ☐
Are guest computers connecting to the network not automatically part of your organisation's security?	no ☐	yes ☐
Are your IT systems unprepared for if/ when there is a breach?	no ☐	yes ☐

Insight