Key elements of a good security solution

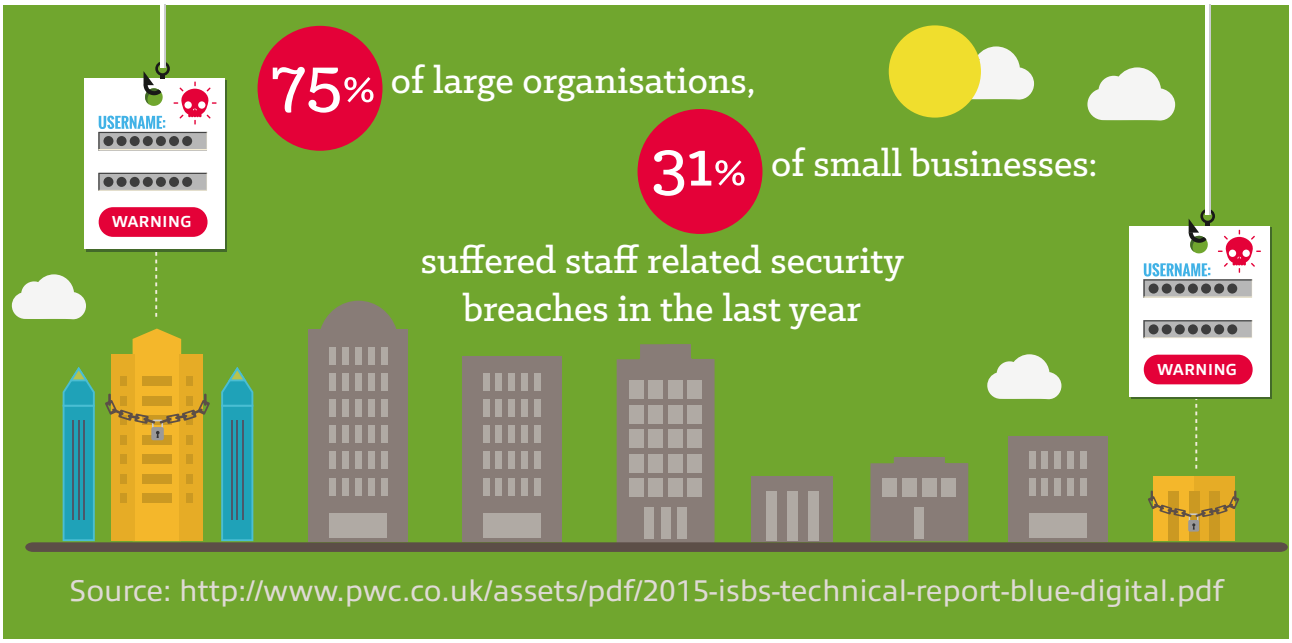
The impact of a cyber attack or other security breach is felt not just in the corporate IT department, but throughout the business. That is why it's vital to ensure your business data and systems are protected by an end-to-end solution that covers the complete security continuum.

By understanding the full spectrum of a robust security solution, the better prepared you will be to close any loopholes and fully protect your organisation against fraud, theft, sabotage, etc.

Selecting a comprehensive solution is not an easy task and the impact of not choosing the right option, that aligns to your individual requirements can be too costly for your organisation.

Based on a consultative approach, a complete security solution should include a range of services and technologies that are designed to drive organisational growth, improve resilience and manage costs.

In alignment to these items, a security solution should also drive Digital Transformation and innovation, whilst protecting your assets and reputation.



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

The following questions highlight some of the key elements to consider when reviewing your security. If you answer "no" to any of them, you aren't as prepared as you could be to minimise risk and mitigate the impact of a breach.

Top **5** questions:

Does your security solution consist of multiple modules from best-of-breed security vendors and "niche" specialists?	no ☐	yes ☐
Is it based on a "defence-in-depth" philosophy?	no ☐	yes ☐
Is it agile enough to rapidly adapt to company change and meet new and emerging threats?	no ☐	yes ☐
Do you incorporate a full range of prevention technologies: firewalls, intrusion prevention, encryption, network access control, two-factor authentication?	no ☐	yes ☐
Do you incorporate a full range of detection and mitigation technologies: anti-malware, intrusion detection, network sensors and intelligent alerting, quarantine features?	no ☐	yes ☐

Insight