



Cyber Crime

Managing Cyber Risk In Your Organisation

Be Aware - Cybercrime in 2016

More attacks seeking financial gain

- Cybercrime is now highly mechanised, hacking toolkits can be readily obtained leading to an increase in the number of perpetrators and attacks.
- Cybercrime is (evolving from "hacking") into a direct focus on power and financial gain.
- Double whammy – more attacks and worse outcomes.
- 90% of breaches are due to human error.
- Attacks designed to coerce people to bypass security.

Review Your Processes

People are now the primary focus of attacks

The current focussed attacks via email and telephone are designed to coerce your people into bypassing security systems by revealing passwords or clicking/opening attachments to authorise access to your systems.

Test your externally facing procedures - do your people know how to identify and deal with suspect communications? You could carry out a "mystery shopper" exercise yourself or engage a cyber specialist to do this for you.

Do your people have a healthy scepticism and a framework for identifying suspect communications? Changes in time, format, language and type of contact can be subtle and training may be needed. As criminals improve their technique so must we to stay ahead.

Educate, Educate, Re-Educate

Over 90% of breaches are due to human error

As this risk evolves our peoples existing knowledge and training may not meet the challenge.

Look again at your company procedures and training agenda, particularly relating to handling of finances and permitting access to IT and physical resources.

Make sure you have an up-to-date cyber security policy which reflects the risk to your organisation. Policy should be regularly reviewed and considered in conjunction with your other processes.

Review and Maintain Technical Security

I've got AntiVirus – isn't that enough?

Maintaining the technical layers of protection is more relevant than ever. Minimise your attack surface by utilising multiple protection layers configured to best practise. As above, your Cyber Policy should be regularly reviewed and developed vs the latest threats.

For clear and trusted
business IT advice call:
01484 779 020
www.p2tech.co.uk



Technologies
Your IT Department. Outsourced.