Cyber Security Checklist

Nautilus House
Redburn Court
North Shields
NE29 6AR

Phone: +44 (0) 191 432 4123
www.wolfgroup.co.uk
E mail: info@wolf-consultancy.co.uk

For enterprises that are highly digitized, more increasingly, performance is dependent on the smooth functioning of computers; the words 'Malware' or 'viruses' could therefore be some of the most dreaded words they hope never to hear.

A recent study suggests that fewer customers of businesses that have suffered information loss are remaining loyal to that organisation, with data breaches causing individuals to take their custom elsewhere. Could you deal with these sorts of losses within your business?

In light of this, we ask how better businesses can protect themselves from malicious attacks on clients' personal data? Using Wolf's security expertise acquired from years in high-security banking industries we've compiled a checklist of our top five recommended practices for securing data and preventing breaches:

1 **Ensure your organisation has an up to date firewall.**

✓ Technology is constantly evolving and so are the ways in which hackers attempt to gain access to your computers. Ensuring your business is using the latest firewall will lessen your chances of an attack by deflecting any information it perceives to be a threat.

2 **Virus software that is current.**

☐ Make sure all of your computers have virus software that is current. As new viruses, worms and Trojan horses are identified daily it's important to know that you're using antivirus software that can automatically update itself. If its list of viruses is out of date, your computers are at risk of an increasing amount of threats every single day!

3 **Get an external company to run tests to verify the 'hardness' of your security.**

☐ Applying a firewall and antivirus software is a step in the right direction, but ensuring your security measures are robust enough to resist an attack is even better. A good IT company will be able to measure your software resilience and offer advice on how to stay one step ahead of potential hackers.

4 **All customer facing servers must be updated with the latest patches.**

☐ A patch is a piece of software designed to update a computer program or its supporting data; fixing its vulnerabilities and other bugs for example.

5 **Get wise to internal attacks. Most security attacks are from within.**

☐ Make sure employees can only access the data that they need, that a strict password renewal policy is in place for users and system's accounts and revoke access rights of ex-employees quickly.