How to safeguard your business from cyber crime?

The threats faced by businesses are from cyber attacks by highly evolved criminals, many operating with relative impunity of prosecution. The risk to organisations can be multi-faceted, with attack vectors such as malware, viruses, ransomware, social engineering and the numerous other commonplace threats.

Whatever the maturity or the size of a business, there are practical things they can adopt to build stronger defences that can reduce the risk and impact of a cyber attack.

Assessment

Many organisations may not fully understand the threats to their business. An independent assessment would help them evaluate their current risk posture, which is offered by many cyber security companies.

Develop a cyber hygiene strategy

A plan should be formulated to address current policies, procedures and budget, as well as staffing and technology improvements. No matter the size and maturity of the business, a cyber hygiene plan should be considered essential if the risk of a cyber attack is to be effectively controlled.

Effective controls

Additional controls may be required to mitigate the risks identified by the assessment. If the business does not have the skills to identify the type of controls and technologies required, they should seek trusted, external advice to ensure the right controls are implemented.

> **"Businesses need to ensure their employees understand how cyber criminals operate and how staff can be manipulated."**

Staff training and awareness

Cyber criminals are experts at exposing a point of entry into an organisation's computer system or through its network. Businesses need to ensure their employees understand how cyber criminals operate and how staff can be manipulated. Regular cyber security seminars and computer based training sessions are essential.

Effective regular patching regime

Out of date applications are more susceptible to malware and cyber attacks. These can lead to an attacker penetrating an organisation's network and instigating a data leak that may cause significant reputational damage. All applications should be checked on at least a weekly basis. Consider implementing a vulnerability management solution that can check for vulnerabilities and apply missing patches.

Create and test an incident response plan

Whatever protective controls are implemented they can never fully mitigate the risk of a successful cyber attack. Businesses should plan for the worst-case scenario by deploying a well thought-out and robust incident response plan that outlines an effective reaction to a cyber attack. The plan should be regularly assessed and updated, ensuring any changes to the business are incorporated. Consider the adoption of a framework for policies and procedures: Best practice procedures can be enforced through the adoption of an independent framework such as ISO-27001, Cyber Essentials, NIST or SANS CIC 20. ISO-207001 and Cyber Essentials have the additional advantage of an independent certification process that may be desirable for many organisations.

Conduct regular external security assessments

Once cyber security controls have been implemented, the controls should be independently verified by a specialist company that holds industry standard accreditations such as Crest and Check.

Create a culture of good cyber security hygiene

Perhaps the most important element of any effective cyber security programme is the ability to embed good cyber security hygiene into the fabric of the business. Cyber security should be driven from the senior management and enforced at all levels of the organisation.