CyberPro.

Risk management: Cyber jargon buster

MARKEL®

Cyber jargon buster

Cyber terminology is viewed as an IT/ technical issue, however some of the risk management areas are essential to understand in simple terms and do not require in-depth IT expertise to protect your business.

Here is a quick guide to some of the common terms used for Cyber Risk management.

Are you using **encryption?**

Encryption protects data from people you do not want to see it and ensures that only authorised users can access it. It works by encoding the data, and typically a password or software key is required to unlock or decode it.

Encryption is particularly important for those using portable devices containing sensitive data such as mobiles and laptops, who might be at risk of having them stolen or going missing.

Encryption software comes in many different forms and offers protection under different circumstances – for example you can use full disk encryption which means all data on the computer is encrypted, or you can encrypt individual files when they are being transmitted to a third party. Some software offers password protection to stop people making changes to data but you need to be aware that this may not stop a person reading the data.

It is important to make sure you know exactly what protection you are applying to your data. In the UK, the Information Commissioners Office (ICO) offers guidance on encryption.

Do you use **two factor authentication?**

Passwords are inevitably used on multiple sites and programmes, most users struggle to make this form of security watertight.

Two factor authentication is the process of adding an extra layer of security in order to access a system or file, for example having a username and password, plus an additional piece of information only you would know. Ideally a physical measure such as using a hardware token, mobile phone verification or thumbprint as part of the process makes password loss or theft less of a threat.

It should be used where there is a significant risk that unauthorised access would leave your critical business operations or data compromised.

Do you use **penetration testing** to evaluate vulnerabilities?

A Penetration Test or Vulnerability Scan refers to the authorised testing or ethical hacking of a network to find potential vulnerabilities.

Security measures can then be put in place in order to better secure the network.

During pen testing usually you would have a simulated attack/security breach with the aim of removing any weak spots.

Do you know if you are using **security patches and supported software?**

Don't be an easy target - using security patches and supported software is the best method of resistance against low level cyber-attacks that work by removing vulnerabilities in an operating system and/or software.

For SMEs with limited IT infrastructure this should be quick and in most cases software can update by default.

Have you considered whether all of your software remains supported?

Software companies do not provide support indefinitely – famously Windows XP which was left vulnerable yet widely used within the NHS. Check if you are using such unsupported software as you are at an increased risk of being the victim of a cyber attack – the clue is usually the vendor trying to persuade you to upgrade to a newer version!

What are **Cloud providers?**

A service provider who offers to host customer's software, services or storage via a data centre that is accessed online.

Many companies use cloud providers, as it has become cheaper to use their capacity and managed services. But like any form of outsourcing you are trusting a third party with your business data that you are still ultimately responsible for, and they may use terms and conditions to limit their liability against you or your customers.

It is important to remember that in the event of data being lost or hacked, you are responsible for that data regardless of a third party cloud provider.

Have you got **Cyber Essentials?**

"Cyber essentials" is a government backed, industry supported scheme launched in 2014 to help organisations protect themselves against common cyber-attacks. In some cases this is a minimum standard to bid for UK government service contracts.

The scheme sets out a series of security controls that help you stay cyber secure, and there two forms of certification – cyber essentials and cyber essentials plus.

You can find out further details of how to obtain cyber essentials here:
https://www.cyberaware.gov.uk/cyberessentials/get.html

Do you train staff on how to spot **phishing scams and social engineering?**

Phishing attacks are increasingly one of the top security challenges for both individuals and companies of all size.

There are various techniques that are used by attackers such as embedding email links that redirect to unsecure websites, attachments containing malware, sending "spoofing" emails where the email appears to be from a reputable source, or impersonating a known company contact.

As Cyber Crime becomes an industry, criminal techniques quickly evolve to maximise the success rate.

Social engineering is a term used to describe the added layer of deception commonly used to add authenticity to a phishing attack, for example a phone call or email style to mimic the person sending instructions.

Educating your staff with training sessions on how to spot attacks and ensuring they are aware of the risks the businesses face from "phishing scams" is vital to your overall cyber security.

What is difference between **data and sensitive data?**

Under the Data Protection Act (1998) "personal data" is data that relates to an individual which can be used to identify that person. Sensitive data can be defined as data held that contains information regarding an individual's:

- political opinions
- religious beliefs
- health
- sexual health
- criminal records

For most organisations financial data will also be considered sensitive (both customer and employee). It is important to recognise the risk to your business if sensitive data is lost, stolen or corrupted.

Have you made preparations for **GDPR?**

In May 2018, this current set of data protection laws will be superseded by the "General Data Protection Regulation" (GDPR) which will strengthen and update the Data Protection Act (1998).

Changes will include amendments to how data can be collected and processed, and the rights individuals will have in regard to the data that a business holds on them (including timeframes to respond and fees).

It is important that all businesses recognise the importance of the GDPR and take appropriate steps to prepare for it. The ICO has guidance on how to prepare which can be found online here:
https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

Do you know what **PCI DSS compliance** is in UK?

PCI DSS stands for Payment Card Industry Data Security Standard.

These are international standards set by the payment card industry that govern how card data should be secured. If a breach does occur anyone who accepts transmits or stores cardholder data failing to comply with the standards risks being subject to the following:

- fines
- card replacement costs
- costly forensic audits
- brand damage or other interruption to business operations

Have you trained staff on **cyber risks?**

Most data breaches arise out of human error, by training your employees to be aware of cyber risks you can significantly reduce the chances of you being the victim of a cyber attack or data breach.

For example:
Do you make sure employees are aware of the importance of having secure passwords?
Do you make sure employees reflect on whether a link or attachment in an email is suspicious before opening it?

Here are some links to checklists and training that will help you ensure employees consider cyber risks at work -
https://ico.org.uk/media/for-organisations/documents/1606/training-checklist.pdf
http://www.nationalarchives.gov.uk/sme/rfi-sme-2017.ppt