RANSOMWARE AND PROTECTING YOURSELF WITH BACK-UPS

Ransomware has proliferated in the last two years and remains an easy and unsophisticated form of Cyber Crime, whereby the criminal encrypts your files.

A typical ransom demand is requested within 48 hours and is aimed lower than the cost/aggravation of being locked out – however the perpetrators are increasingly less willing to unlock files and may simply increase the ransom to extract further.

The attacks can be made via website and software vulnerabilities, but in the majority of cases they are email born attachments or links, so the human error factor is more difficult to eliminate.

Back-ups are the most effective form of resilience to avoid the cost and disruption, and furthermore ensure the criminals are not rewarded. There are degrees of complexity to ensure your back-ups are not also encrypted by the malware, and to have capabilities to mirror or roll back your network with minimal disruption.

Emerging risks are ransomware attacks on mobile phones and social media accounts where the personal impact can be greater.

Why it Matters

Despite all our best efforts some cyber-attacks will succeed. When our defences fail and an attack succeeds, we must ensure that we can cope. One of the best ways to do this is to have a robust backup regime that is protected from the attack. This is especially true of ransomware attacks that specifically seek to encrypt your data and to extort payment from you to get it back.

In any event backups can help mitigate against a wide range of potentially catastrophic problems, such as fire, theft and flooding and malicious insider attacks.

Key Takeaways

- Backups shouldn't be seen as the primary defence against ransomware. Backups are a last resort, rather than a primary protection.
- Identify all your key data stores.
- In each case make sure you have a regular (at least daily) backup.
- Ensure you take regular offline backups to give maximum peace of mind.
- Do not keep backups on mapped drives as these can be targeted by malware.
- Make sure the security around your backups is strong.

Getting the Basics Right

Data Mapping

If you are going to have a backup strategy to protect against cyber-attacks then the first thing you need to know is where your critical business data is kept. For many small businesses this will vary between shared drives, local stores on devices and third party providers.

You should first categorise your data by answering a few basic questions:

- **What are your personal data categories?** For example: employee, contractor, customer, vendor.
- **Who are the owners?** For example: HR, payroll, pensions, contracts, procurement, customer services.
- **What are your data sub-categories (or elements)?** For example: name, address, date of birth, financial records.
- **What format is it in?** For example: emails, forms, letters, spreadsheets, application data or database records.
- **Where is the data stored?** For example: local device, database, application, cloud hosted or with a partner?

What backups currently exist and where are they stored?

This data mapping exercise is also useful for undertaking cyber risk assessments and compliance assessment against the new data protection rules that comes into force in May 2018 (GDPR) so it's worth investing some time to do this properly.

Determining Backup Frequency - Some data is more valuable than other data and some data is changed more frequently than other data. These are the kind of issues that must be taken into account when deciding how often to backup data. The criticality/value of the data should determine how frequently it is backed up. Storage is relatively inexpensive these days so it may be possible to simply back everything up online nightly and offline weekly.

Dangers of permanently mapped backup drives – Many businesses simply map a shared drive and use it as a backup share for everything. This is dangerous for two main reasons: firstly ransomware targets mapped drives so this will not offer any protection and secondly it provides a single weakly-secured location where all data is stored, useful for any hackers or insiders looking to steal it.

Check your backups really work – Configuring backups can lead to a false sense of security. If you are going to rely on them you must ensure they are actually backing up the data you need. The only way to be sure is to check the backups regularly – especially if you change any software as this may lead to backups ceasing to work.

Third Parties – Of course it may be a service provider or key supplier that gets attacked. The critical data may be in their control. You need to check what their backup strategy is for any key suppliers and furthermore arrange for a regular export or transfer of your data as a last resort. A data escrow service may provide a solution.

Protecting your backups - Any file system that's attached to an infected machine is potentially vulnerable, as well as attached external hard drives and plugged-in USB sticks. To make your backups ransomware proof, you should use a drive not mounted to a particular workstation. For example, stream the data over the network to another workstation or storage device using a backup application/agent. This storage device should not be accessible to user workstations.

Security controls need to be in place to segregate users from backups. Off-site well-secured and encrypted backups are also a good practice.