Avoiding the dreaded ‘headache’ of managing your data.

How to protect your data more effectively and reduce the risk of costly data loss.

Microtrading
Your trusted IT partner

43% of organisations without a data recovery and business continuity plan cease trading following a major data loss.

Data protection and recovery are business essentials.

We live in a 24/7 global economy that is more dependent on technology than ever before.

The desktops, servers and mobile devices of sporting organisations and their members contain a variety of sensitive digital data, including:

- Employee and member information
- Internal emails
- Documents and financial records
- Sales orders and transaction histories

The above are all examples of data that an organisation cannot afford to lose or have exposed. This applies equally to applications and programs that are critical to daily operations and services.

How costly can data loss or a data breach really be?

While corporate-level data losses are well publicised, many sports and non-profit organisations mistakenly believe their data isn't at risk.

This mistake can prove to be a costly one. A single data breach or data loss event can be devastating to a sporting or non-profit organisation, with ongoing expenses causing serious problems.

Internal research and investigation into the event, system repair and maintenance, and data security protection amount to a heavy price. If cybercrime is involved, affected members must be notified and there is a potential for litigation. This damages the relationship with the member and can lead to losing them entirely.

Revenue is also lost if employee productivity and member accessibility/ service are significantly impacted.

The threats posed by cybercrime and technology failure are serious, but they can also be effectively mitigated through proactive management of your IT and data. In this guide, we identify the areas that need to be properly taken care of, to create a healthy IT security culture and protect systems and data against a catastrophic event.

Following a significant data loss, it is estimated that small organisations can lose up to 25% in daily revenue by the end of the first week.*

- 50% have gone into administration immediately.
- 93% of organisations that have experienced data loss, and prolonged downtime for ten or more days have gone into administration within twelve months of the incident.
- 43% of organisations with no data recovery and business continuity plan cease trading following a major data loss.

*Data from Unitrends Inc, a US-based company specialising in backup and business continuity.

Why do I need to enforce a data security strategy?

It's no good creating a security strategy if it is not going to be properly implemented.

It's important to manage the 'human factor' of data security through guidelines and training. This must include communicating data protection policies to staff and members and ensuring their implementation. To enforce your security policies, rules must be set – particularly for use of personal devices.

It can be as simple as sending reminders explaining not to open email attachments from unknown sources, establishing a password etiquette or the restriction of specific filesharing or social networking sites.

As part of this, you should also stress the importance – both for the individual and the organisation – of properly protecting sensitive and personal data.

Do I need to regularly review my data security policies?

Threats to IT are everchanging, be it trends in user behaviour or the tactics of cybercriminals.

As a result, your data security policies need to be an evolving set of guidelines – adjusting and growing to respond to such changes.

Over recent years, to protect its data security, IBM has put a variety of bans and restrictions in place for those that enter its premises or access its systems. These have included restricting the use of cloud storage services, Siri – the iPhone personal assistant, and USB sticks.

If a company of IBM's size can go as far as making such demands of its extensive employee-base, a sporting organisation can implement similar rules on a significantly smaller team. As such, feel free to remind an employee or member that they are not to play Fortnite on a laptop that contains organisation and member data.

What is mobile device management?

Mobile device management enables sporting organisations to effectively control the mobile devices used within the organisation. This makes BYOD (Bring Your Own Device) as safe as possible, both for individuals and the organisation.

Devices tapping into the organisation's systems are identified, remotely monitored and managed 24/7. More importantly, they are proactively secured via specified password policies, encryption settings and automated compliance actions. In addition, any lost or stolen devices can be located and either locked or stripped of all organisation-related data.

Data backup and snapshots

Fully backing up large amounts of data can be a lengthy process. The data being backed up is also vulnerable to file corruption from read errors. This means sizeable chunks of data may not be stored correctly in the backup file and would be irretrievable in the event of a full restore.

Snapshots are a great way to comprehensively back up your organisation's most critical data. Snapshots are read-only copies of data, frozen to a specific point in time and stored using minimal disk space.

By creating snapshots incrementally, you'll have the best backup coverage possible of the data you need with the resources you have. These virtual snapshots are immediately available for restores in the event of data loss.

It also goes without saying, you should regularly perform test recoveries from your backups so that you understand how long the recovery process takes and have proof that your data can be comprehensively restored. From our experience, not enough organisations test their backup solution and verify it is working as expected!

Cloud replication and disaster recovery services

Cloud storage and hosting is ideal for sports and non-profit organisations who may consider data backup to be too costly, time consuming and complex.

The cloud offers a cost-effective, automated off-site data replication process that can provide continuous availability to business-critical data and applications. Cloud replication can often get systems back online in under an hour following a data loss event.

How can Microtrading help?

As a Managed Service Provider, Microtrading offers a proactive IT service that makes its clients less vulnerable to cyberattack and helps them to prevent catastrophic loss of data or systems.

We can help you to create an effective data security policy that works by:

- Advising on and implementing the migration of systems and data to the cloud
- Providing cyber security awareness training to empower your staff
- Proactively managing all sensitive data, and the users and devices that access it
- Constructing and overseeing a comprehensive backup and disaster recovery strategy

Microtrading
Your trusted IT partner

For more information on how Microtrading can help, **call 0121 784 0077 or visit www.microtrading.co.uk**