RISK INFORMATION – CHURCHES
CYBER SERIES - BACKUP

Churches are increasingly dependent upon computers for efficient operation of their administrative functions and ministry activities. The non-availability of computer programs and related data can have a significant negative impact on a church ministries.

To help mitigate the impact of lost or damaged data and/or programs, it is important that extra copies are kept of all key systems and data. These extra copies are referred to as backup.

Backup can provide an organisation with the ability to continue processing with the minimum loss of functionality and data.

The information provided in this publication is intended to assist churches understand the need to create and maintain backup copies of data and programs.

Why does my church need to backup?

Backup is needed in order to help restore processing capability to an organisation. To this end, backup should include both programs (systems) and data.

A church will need backup because sometimes things fail. Causes can include failure of storage devices (e.g. disks) or some other hardware component.

Software may fail because it has not been kept up to date – manufacturers' changes or patches may not be applied or may not be applied in a timely manner.

Currently, society has experienced a surge in attempts to exploit and infiltrate computers connected to the internet. Examples of such activity go by the names: virus, Trojan horses, malware etc. The purposes of such activity are varied, including: theft of commercially sensitive data; obtaining personal details of individuals (identity theft); to access value (bank accounts and the like); to hold organisations to ransom and demanding payments; at other times the objective may be malicious intended only to stop a computer system from operating.

When a church attempts to recover from an attack, the availability of backup data may help a church from having to start again from scratch.

The information provided is of a general nature only and may not identify all matters that need to be included in the design of effective controls for the subject area. Professional advice should be obtained on individual circumstances.

RISK INFORMATION – CHURCHES
CYBER SERIES - BACKUP

What should our church backup?

All programs and data should be backed-up.

Programs should be backed up when new programs are acquired or existing programs are changed, e.g. following application of vendor updates.

Backups should provide the church with the ability to restore data to a point as close to the current date as is possible.

Backup will include full copies of all data and may be supplemented by more frequent copies of changed data.

How frequently should our church backup?

The frequency of data backup will be influenced by the importance of the data to the organisation and the frequency of changes to the data. For example, data that is changed once per annum requires less frequent backup than data that changes daily.

As a minimum, we recommend that all data should be backed up weekly. Where there is a large volume of data processed, more frequent back-up (e.g. daily) may be required.

Where you are using a computer service operated by a third party supplier (e.g. accounting packages such as Xero) ask the supplier to provide you with a written explanation of their back-up regime.

Where should backup copies be kept?

As a general principle, backup should be on media other than that used for storing operational data files. Use could be made of "cloud" based backup, separate from where operational copies of data are stored. Some churches may consider establishing a separate copy (or "ghost") of their main data storage to facilitate prompt recovery from service interruptions.

Consider keeping one backup copy offline, e.g. the copy is held on a removable or portable hard drive. The most recent backup copy should be stored offsite to preserve your church's ability to continue processing in the event of physical damage to computer facilities and/or network.

A minimum of 3 generations of backup data should be kept, i.e. the current copy and 2 previous copies.

The information provided is of a general nature only and may not identify all matters that need to be included in the design of effective controls for the subject area. Professional advice should be obtained on individual circumstances.

How do I know it works?

Organisations need to ensure that their backup is effective, i.e. that it works. This will normally involve practicing the process of restoring data from backup copies. Care needs to be taken in this process that operational programs and data are not impacted.

Churches may need assistance in undertaking this check.

What about encryption?

If operational files are encrypted, backup procedures will need to consider whether the backup is also to be encrypted or data is to be kept unencrypted. If backup data is encrypted the restore processes need to include the capability to unencrypt.

When backup is taken offsite, we recommend that the files be password protected and/or encrypted.

How will we know what to do?

Your church should have a written plan outlining how and when to backup programs and data. The plan should also include details of how to recover or restore date. It will outline the different roles to be undertaken by staff, volunteers and external service providers.

Plans should consider responses to a variety of scenarios including physical damage, hacking etc.

For more detail refer to the publication: BIS Cyber Series – Data Breach Plan

What about insurance?

Lack of effective backup may compromise your churches ability to claim restoration costs under cyber insurance.

Third party access to unprotected backup data (not password or encryption protected) may render cyber insurance ineffective.

The information provided is of a general nature only and may not identify all matters that need to be included in the design of effective controls for the subject area. Professional advice should be obtained on individual circumstances.