## What is it (for this example back up)

In terms of cybersecurity, Backups are the last line of defense for organizations to be able to recover their business in an event where their systems are compromised, crypto lockers or maliciously deleted by adversaries. Being able to recover your data reliably is an essential part of any Disaster Recovery and Business Continuity planning.

The critical parts of backups are:

* Ensure all critical data is backed up and there is nothing critical to the business missing
* Ensure there is a report generated to check that backup of all components has been performed
* Ensure that the backup of the data is set up for immutable storage which means that backup systems are disconnected after backup is achieved to ensure that they cannot be compromised.
* Ensure backup is tested by restoring data from back on a regular and scheduled basis

## Recent examples of where things can go wrong without suitable backup solutions:

*Lake City, Fla - More than 100 years’ worth of municipal records, from ordinances to meeting minutes to resolutions and City Council agendas, have been locked in cyberspace for nearly a month, hijacked by unidentified hackers who encrypted the city’s computer systems and demanded more than $460,000 in ransom. Ref The New Yor Times* [*https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html*](https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html)

Don’t let this happen to your organisation. You need to ensure that your last line of dense is enabled and tested with assurances provided to your executives and board.

## User Case - Example of where your organization may require Fortify’s backup advisory service

You have been asked by your organisation’s Audit &Risk Committee to provide a report on the status of the backup systems and the ability to recover the business in case of a major disaster such as being exposed to a ransomware attack.

You think your IT person is performing basic backup services but there are no reports generated and there are no guarantees that the backed-up data is accurate or that all your critical data has been backed up. To add to your woes your IT provider can not supply information on whether the backups have been tested or if your backup data will not be affected during an attack where adversaries attempt to encrypt all systems.

You need to get professional assistance to solve the critical parts of the backup as described above, but it sounds expensive and being a small not-for-profit organization, you have a very limited budget to get this done. You are also not aware of whom to approach and how to go on about engaging a consultant to help you achieve what is required.

## Where Fortify can help

Fortify is a not-for-profit organization with cybersecurity expertise, resourced by volunteer professionals. We provided Cybersecurity advisory services at minimal, or at no cost, to assist organizations such as yours that have limited resources.

Fortify will provide a self-assessment guideline and questionnaire so you can assess your requirements in this area.

Depending on your needs we will then assign a professional consultant to review your backup environment, perform an audit of what is backed up and provide a report on how to improve.

We may be able to assist you in configuring your systems to achieve the desired results, however, if a new solution is required, we will then assist you in architecting and scoping a go-to-market procurement activity to acquire solutions partner if required.

## How to engage Fortify

There are a few simple steps to follow in engaging our services

1. Go to the website: fortify.com.au
2. Register your organization
3. Read the guidelines and start to complete the self-assessment questionnaire. Please allow 50 minutes to complete the questionnaire as some areas may be complicated and require some careful thought
4. If you required assistance to complete the questionnaire, please submit a request via the “require assistance” button or go to fortify.com.au/assistance.