

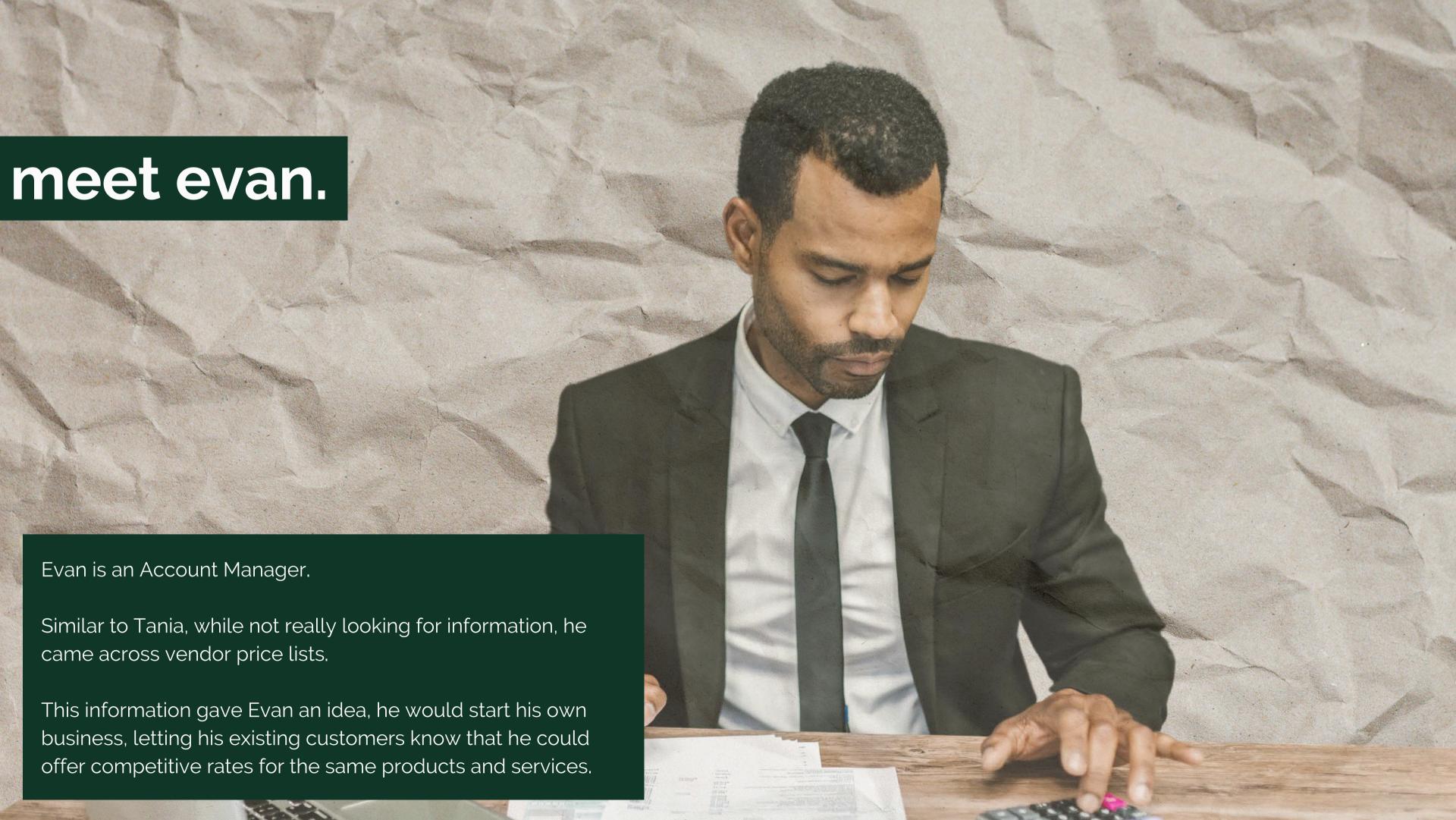
MYRTEC PRESENTS

DATA STRUCTURE & PROTECTION

Safeguard your data from internal or external threats or theft





















what will happen if your data gets breached?

- fines
- legal action
- reputational damage



strategy

- prepare, because a data breach is a 'when' not an 'if'
- develop a plan that will help you limit exposure, liability and risk
- understand compromise commonly occurs through the breach of a user account, therefore the less data that each individual has access to, the better



using the right tools

- set company level permissions using sharepoint or shared drives
- avoid using tools with individual led permissions such as one drive or google drive
- azure virtual desktop



data structure

- data structure should be based on your org chart
- policies must be configurable per silo e.g. data loss prevention, retention policies and sharing policies



building access control

- roll-based permissions
- principal of least privilege



rationalisation of data

- bring all your data back into a structured and controlled environment where data can be monitored, managed and have policies applied
- this environment can have a system policy or a written policy



reducing surface risk area

- single copy of data
- blocking USB's
- blocking drop box
- blocking sharepoint sync



policies

 you can opt for system or written policies but ideally you should be using aligned written policies around privacy and data usage by employees



benefits

- efficiency
- avoid shadow IT
- extends beyond data structure
- power automate / workflow
- co pilot / gemini







thank you for joining us.

Email

hi@myrt.ec

Phone

02 9146 6330

Socials

@myrtec

Website

myrtec.com.au



