MYRTEC PRESENTS

DATA STRUCTURE & PROTECTION

Safeguard your data from internal or external threats or theft

case study:

Suits Solicitors

Suits Solicitors is a Newcastle-owned and operated law firm.

They have an IT provider but haven't evaluated their security posture in years. This is because Senior Management believes their IT systems are 'working' and they can't see the value in investing time or money into security when they already pay for an Antivirus solution.

meet tania.

Tania is a Lawyer at Suits Solicitors.

One day Tania was clicking through documents in SharePoint looking for the company work from home policy.

While in the HR folder, she found old pay slips which indicated how much her co workers were earning,

Tania was frustrated by the pay discrepancies in the office and started gossiping with other co workers about details which should have remained confidential.

meet evan.

Evan is an Account Manager.

Similar to Tania, while not really looking for information, he came across vendor price lists.

This information gave Evan an idea, he would start his own business, letting his existing customers know that he could offer competitive rates for the same products and services.

meet viv.

Viv has worked at Suits Solicitors for over twenty years in an Admin role. She has access to all files and folders as she does all sorts of extra jobs around the company and never knows when she will need certain documents.

Viv's computer was compromised when she clicked on a dodgy link prompting her to reset her Microsoft password.

The hacker got into her computer remotely and downloaded the data to sell on the dark web.

meet kevin.

Kevin, a Partner at Suits Solicitors, thought he was being responsible by holding on to old data in an archived folder because “you never know when you might need it.”

This archived data included confidential details such as clients payment information.

When Viv was breached, all of this data that he was holding onto unnecessarily also went to the hacker.

what could have been done differently?

tania.

If Suits Solicitors had a proper data structure in place, such as a **secure location to store sensitive information**, Tania would have only been able to access the HR workplace policies that were relevant to her. Other documents in the HR folder, such as pay slips and leave applications would have remained confidential.

evan.

Suits Solicitors should have had a **tiered security level system** in place. So while Evan may have needed some documents in the Accounts folder such as client names and details, he wouldn’t have access to price lists.

viv.

Staff should **only have access to the systems they require to complete their role**. Anything else ad-hoc should be granted access on a case-by-case basis. It's not a matter of whether the staff member is trustworthy, but limiting area of exposure from a breach.

Of course training is also recommended to prevent accidental handover of data.

kevin.

Suits Solicitors needed a **secure archive space for legacy data**. This means that it has heavily restricted access, a retention policy put in place and a secure location to store it all in.

They should have also only held on to relevant data, such as case notes, and not private information such as payment methods.

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

q&a

thank you for *joining us.*

Email

hi@myrt.ec

Phone

02 9146 6330

Socials

@myrtec

Website

myrtec.com.au

myrtec