DP COMPUTING

8 STEPS
TO PROTECT YOUR COMPANY DATA
WHEN PEOPLE LEAVE

www.dpcomputing.com.au

Businesses owners would like everyone to be a big happy family with very little or no turnover, but that is not always possible. When employees leave, you may be opening the door to a data leak or compliance risk.

This eBook shares what you need to know to better secure your business when someone leaves or is let go.

When your staff leave, your data should not leave with them

Employee turnover can be costly for many reasons, including:

- Business productivity can decrease
- Loss of company knowledge
- Having to recruit and train new staff.

Have you thought about the risks around your data?

This eBook shares some steps you can take to help protect your data, including:

- Find out more about the risk when people leave your organisation.
- Explore strategies to prevent turnover.
- Learn how to create a culture of security throughout employee tenure.
- Read about the ways an IT provider can help protect your data.

Understanding IT risks related to employee turnover.

There will always be at least a small amount of employee turnover in any business. The reasons are many and varied and can include younger workers who see greener pastures elsewhere, or older workers ready to retire. Problems though can arise if employees take any sort of company data with them or leave have still have remote access.

When people exit your company, whether on good terms or not, they represent a data risk. With a lot of companies now allowing bring-your-own-devices, they could have company data on a privately owned laptop, tablet or smartphone.

With a lot of people still working from home on their own devices, there may also be questions about what constitutes professional or personal data. Your business may need to consult with a lawyer about who has rights to what data and work done.

Someone leaving involuntarily might deliberately delete data from your company. They could download data to a USB drive or transfer data to a personal cloud storage account. They may release data publicly, sell it to criminals or take it to your competition.

What can you do to offset the risks?

#1 Begin at the beginning

Obviously, you want to hire honest people with the right intentions for your business. When you are first onboarding new employees you need to educate them about data security. Ensure they understand the importance of strong passwords, encryption, and saving information securely. That means using a secure server or using the business's cloud storage rather than saving documents to a local machine.

#2 Provide ongoing training

Regularly train your employees on security and how you would like them to treat your business data.

Discuss what they can and cannot use to access corporate data (especially intellectual property or trade secrets).

#3 Develop a security culture

Onboarding and training prove your business prioritizes security. Also, set clear policies on visibility into employee practices, data encryption and backup.

If you are going to allow people to use their own devices, use remote management to monitor that activity. When someone does leave you, immediately go in and secure or remove company data.

#4 Monitor employee behaviour

Have a clear overall picture of who is accessing what and from where. Knowing what employees use what resources can help you spot questionable behaviours. For example, people regularly download documents or send information to the cloud, but is someone suddenly doing this more than normal? That may mean they are preparing to leave and could be taking data with them.

In the news: *Leica Geosystems in Australia sued an employee for downloading 190,000 files containing sensitive information on his last day at work.*

Why people take data with them?

The three main reasons employees take business data when leaving their employer are:

1. It is done unwittingly as they don't even know that they have data they shouldn't on their personal devices.

2. They don't think they're doing anything wrong. Maybe they did the work to create that data, or they don't see that data as something that is valuable enough to protect.

3. They are not happy. They may be upset about being fired or being passed over for a promotion. They may intend to leak the information, sell it to criminals, or use it to their own personal advantage in their new job at a competitor.

#5 Limit access to data

Having a description of your IT and employee roles can also help you to limit access. Taking a least-privileged access approach is the safest route. This allows someone to have access only to what they need and nothing more. This can help cut the damage if someone inadvertently or intentionally leaves.

#6 Prioritize data protection

Implement policies to force people to save important work to secure locations and ensure you have a good backup in place (and regularly test it to!). This can help you recover more quickly in the event of a malicious attack. It can also be useful if someone inadvertently deletes something important while trying to wipe devices clean for a new user.

#7 Have an exit policy

Your employment contracts need clear language about protecting sensitive and confidential data and regularly reiterate these policies to your staff. If the employee has access to your social media, ensure they are no longer able to log in and post or delete content.

Also, establish a procedure for proper data removal from employee devices. Enlist IT to clear corporate technology and wipe employee personal devices if they leave.

In the news: *Atlantic Marine Construction Company sued a former employee for installing remote access software without authorisation. The employee accessed the company's network at least 16 times after he left to take confidential information.*

#8 Communicate Internally

Make sure all relevant parties know about terminations immediately. If and employee leaves (whether on favourable or unfavourable terms) but IT doesn't know for a week, that could leave you exposed.

Know who needs to know about terminations so that they can remove logins and close accounts. Expect prompt action to change passwords on shared accounts or blacklist terminated employees.

Keeping employees happy helps, too.

Another way to stem disgruntled employees leaving with your data is to engage employees and give them meaningful and enjoyable work and become a place where people want to work. Some strategies to help encourage employee loyalty, while also boosting productivity, include:

Welcome feedback. Make it obvious that you are willing to hear from employees. Then, where possible, act on what the employees say. This shows you respect their input and helps everyone feel more involved at work.

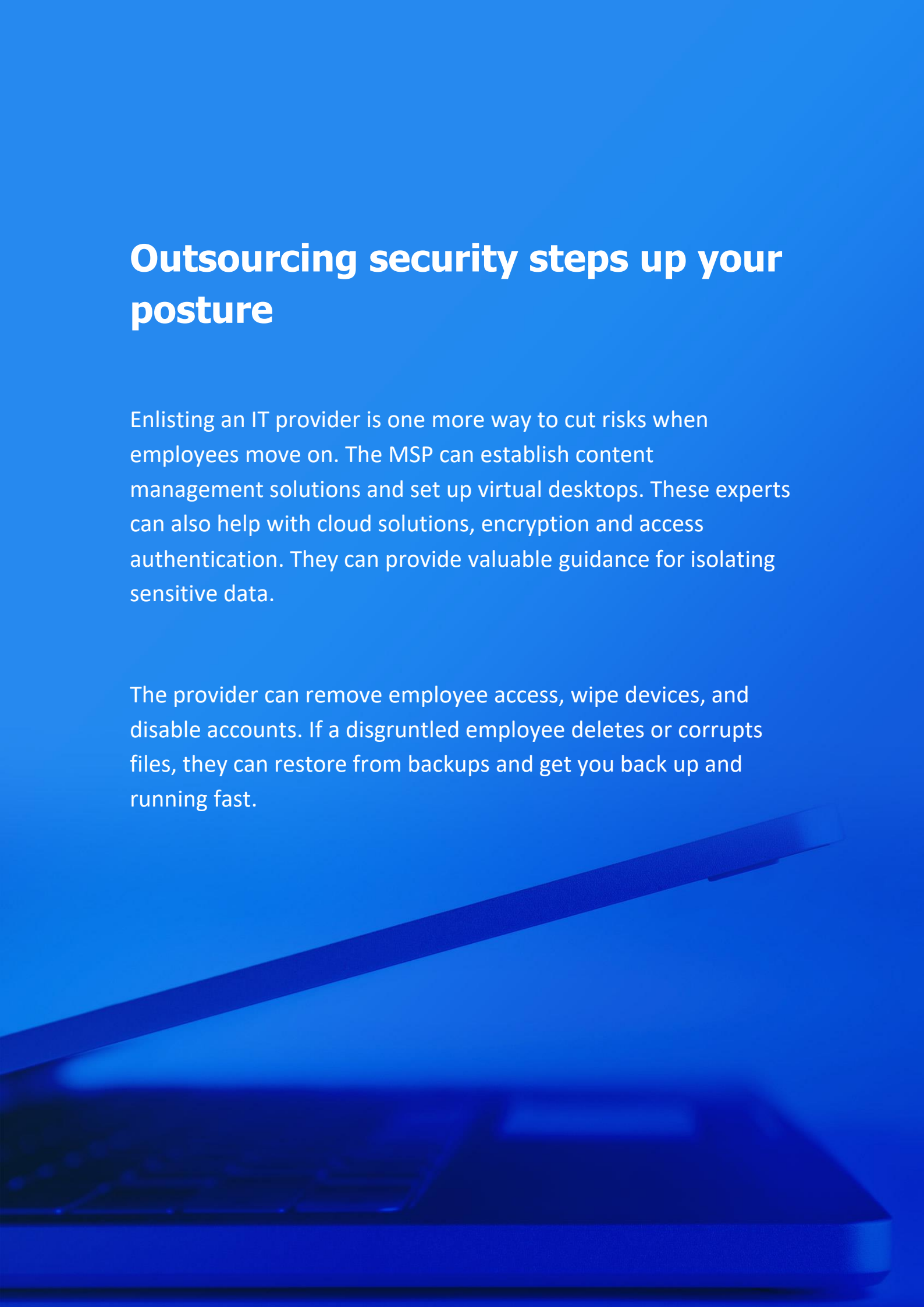
Encourage risk-taking. People like to feel challenged, so they are less likely to look elsewhere to work. Make yours a company where people feel safe trying new things or making fresh suggestions.

Set goals. Help individuals identify challenging areas. You don't want to make the goals too difficult, as that may lead to the frustration you are aiming to avoid.

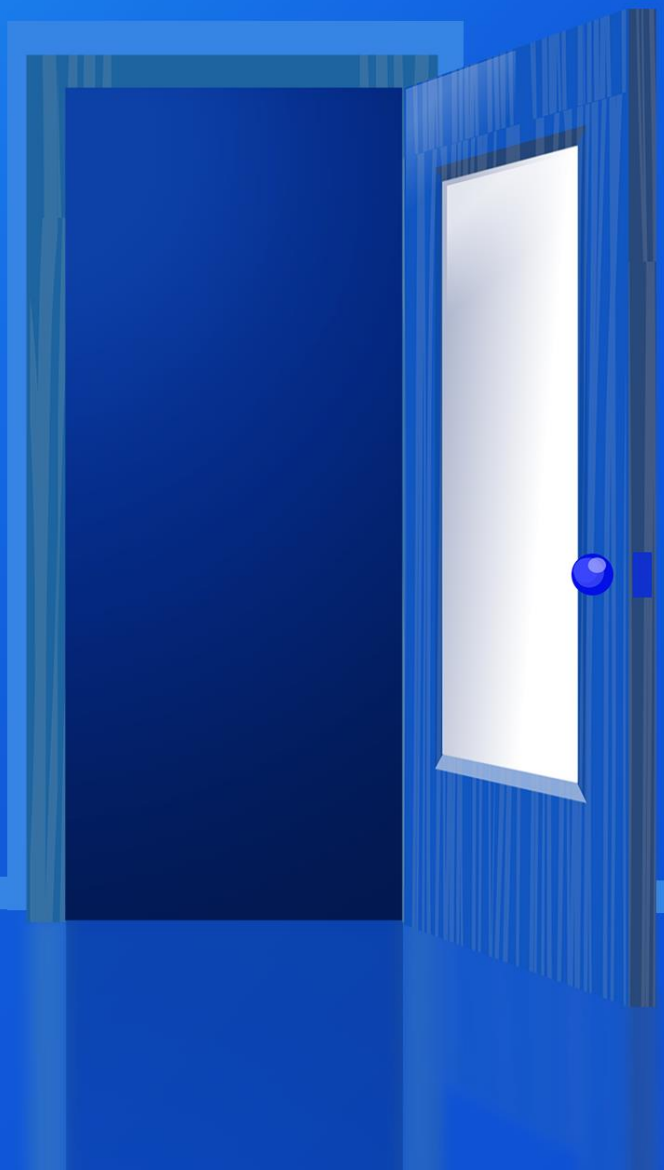
Outsourcing security steps up your posture

Enlisting an IT provider is one more way to cut risks when employees move on. The MSP can establish content management solutions and set up virtual desktops. These experts can also help with cloud solutions, encryption and access authentication. They can provide valuable guidance for isolating sensitive data.

The provider can remove employee access, wipe devices, and disable accounts. If a disgruntled employee deletes or corrupts files, they can restore from backups and get you back up and running fast.



DP COMPUTING



Phone: **(08) 8326 4364**

Email: **support@dpcomputing.com.au**

Web: **www.dpcomputing.com.au**

Facebook: **facebook.com/dpcomputing**