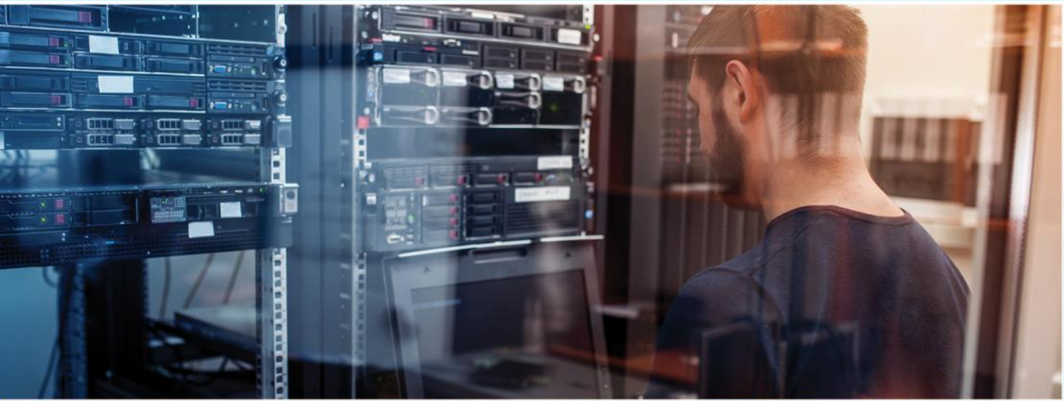
HACKING - A SOPHISTICATED THREAT TO BUSINESS



Hackers have an easy way to scan the internet for all active I.P. Addresses (devices connected to the internet); they can access the known and published vulnerabilities for any of those devices; they have developed toolkits which will automate their search and identification process; they have tools to break into any device connected to the internet and with crypto-currency they can make easy untraceable money.

Hackers - a growing threat for all businesses

Before we elaborate on how hackers operate and how easy it is, here is a real example.

This example business operates a busy office in a region of NSW. Like so many people these days, they relished in the ability to come home from work to have dinner with the family then log back in to the office later that night to finalise some work. Unfortunately, it was the ease of the remote connectivity to the network that also had a terrible backstory to it; namely presenting hackers with the opportunity to gain access to the business's data.

This is one of many similar scenarios occurring daily with small to medium sized businesses. This particular business, through inadequate security measures, unknowingly had a hacker breach their server, encrypt all of their files and then issue a ransom note for around 1 bit coin (at time of the attack, approximately A$8,000.00). The files were largely worthless to the hacker BUT were the currency and life blood for the business. So how did this story end for our real situation business victim? Not too well I am afraid. The ransom was paid but the hackers then went quiet. Now the business has lost their data and the ransom money. They have downsized considerably and relocate back to the home office.

So how can this happen to so many businesses and individuals?

A SOPHISTICATED THREAT TO BUSINESS

Vulnerabilities in the internet

The internet is a hostile environment. It’s an interconnected network consisting of approximately four billion internet addresses. These addresses are called Internet Protocol (or IP) addresses and it is how all communication occurs on the internet, and within every computer network. Behind each IP address can be any number of devices and computers in business or home networks. Many of these devices have vulnerabilities.

Vulnerabilities can take the shape of mistakes in programming, insecure policies by the device manufacturer or deliberate programming of a backdoor. In fact, most vulnerabilities are mistakes in programming. Programmers are only human and are often under a lot of pressure to deliver a product. Hence why we get so many updates to Windows and Mac operating systems each month.

Why would hackers want my data?

They are after your data and information, because it is extremely valuable to you and in some cases can also be valuable for trade on the dark web. Your business data is like currency. Even in a small to medium business, data is just as attractive to hackers as a cash register at a corner store and data is easier to get.

Hackers have two options with your data; they can recognise that its worth more to you than it is to them, encrypt it (lock it up) and hold your business data to Ransom (your work files, your life’s studies etc). They can also recognise that sometimes the data is valuable to them as well, such as your customers’ bank details, credit card numbers, emails and home addresses, Medicare numbers etc etc. The dark Web is a thriving market place for personal details that can make a lot of money for a hacker and can be the basis for identity theft for other unscrupulous operators.

How do they do it?

Anyone with an internet connected computer can attack you. These days, computers are very powerful devices, hackers have learned a lot over the years, they consider their chances of getting caught to be slim and they now have access to some very sophisticated tools. Bruce Schneier, an American cryptographer, computer security specialist, and writer said, ‘attacks only get better; they never get worse’.

The challenge for any hacker is to gain access to your data storage (your laptop, server etc). There are many vectors for infection (placing a malicious software in your system). You can be ‘tricked’ into letting the infection in, for example through spam, social engineering, malicious advertising, or there are ways the hacker can ‘break in’, including website hacking, insecure remote access, insecure communications, aging equipment or vulnerabilities in software or equipment.

But how do they choose which business to ‘hit’? Well, it’s not personal, *its random plus vulnerability*. A hacker can go on any number of public websites that lists every device open to the internet and can apply his or her automation tools to choose targets to attempt to hack into. If you are reading this on your computer right now and you’re on line, your IP address is one of millions around the world that may come up in such a search.

A SOPHISTICATED THREAT TO BUSINESS

They don't know you, they just know your IP address is vulnerable and they will try to exploit it to see if they can earn some money.

There is also Bitcoin and other cryptocurrencies which are digital currencies being used to buy and sell items anonymously on the internet. Think of these currencies as untraceable internet cash. Through crypto-currencies, hackers have a way of being anonymously paid. This makes things even more attractive for hackers.

Hackers don't necessarily have to scan the internet looking for vulnerabilities themselves. They utilise products such as Shodan (like a 'Google for hackers') and Masscan, meaning they can scan all four billion internet IP addresses, looking for vulnerabilities in less than six minutes. If a vulnerability or insecure practice is found, the hacker will look to leverage this into an attack. Rather like a burglar identifying that your house is easier to break into than your neighbour's

The consequences

There can be many outcomes from hackers breaking in and accessing your data including:

- Your data being 'locked up' and held to Ransom. This ends up with the victim either paying the ransom but in many cases the data is not returned anyway (or sometimes the victims choose not to pay).

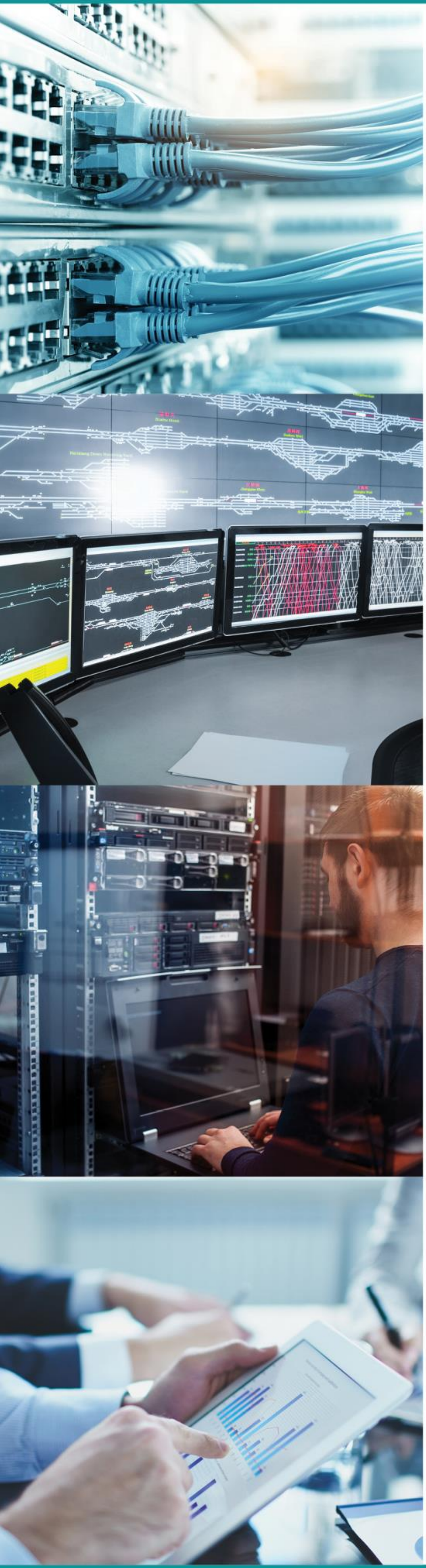
- Your data being stolen and sold to unscrupulous third parties; quite often, you would not even know this happened unless it is your personal details that have been utilised for identity theft.

- There are also risks that you may have breached various Federal codes of conduct by not reporting data theft, and as a real side note, it is an offence to pay a ransom under Australian counter-terrorism laws in which you may be accused of financing a terrorist organisation.

Prevention: keep them out

1. Appropriate Endpoint security.
2. Appropriate protection software for your platform (onsite or in the cloud).
3. Specialist security software for remote connections via a Virtual Private Network (VPN) appliance.
4. Have a bulletproof backup solution in place that is appropriate to your platform (onsite, remote and/or cloud).
5. Have the necessary password management regime.
6. Up-to-date operating software (the older your software and operating system, the more known vulnerabilities).
7. Frequent audits and consultations with your I.T. provider.

A SOPHISTICATED THREAT TO BUSINESS



Why would you use Loyal I.T. Solutions?

In 15 years, our business has a proven track record in providing a full suite of services, from I.T. planning and system audits, onsite and cloud solutions, maintenance, helpdesk and the supply of hardware and software from industry-leading vendors.

Our team of 12 has expertise in technical, consulting, helpdesk and sales. We operate by a Code of Honour and have won several awards for business and excellence in business ethics.

It is our mission to assist you to achieve your goals, by understanding your business and providing the solutions required. In other words, it's our mission, to help you achieve your mission!

5 MORE REASONS TO USE LOYAL I.T. SOLUTIONS

Guaranteed Response Times.
Excellence is our Standard
No Geek Speak
No Lock-In Contracts
Guaranteed Solution

LIKE TO KNOW MORE?

Click **here** to request more information from Loyal I.T Solutions, or give Loyal I.T a call on 02 4337 0700

You may also like some of these fact sheet flyers

- Reliable Back-ups
- Reliable I.T equipment for business
- I.T security for business
- Cloud back-up