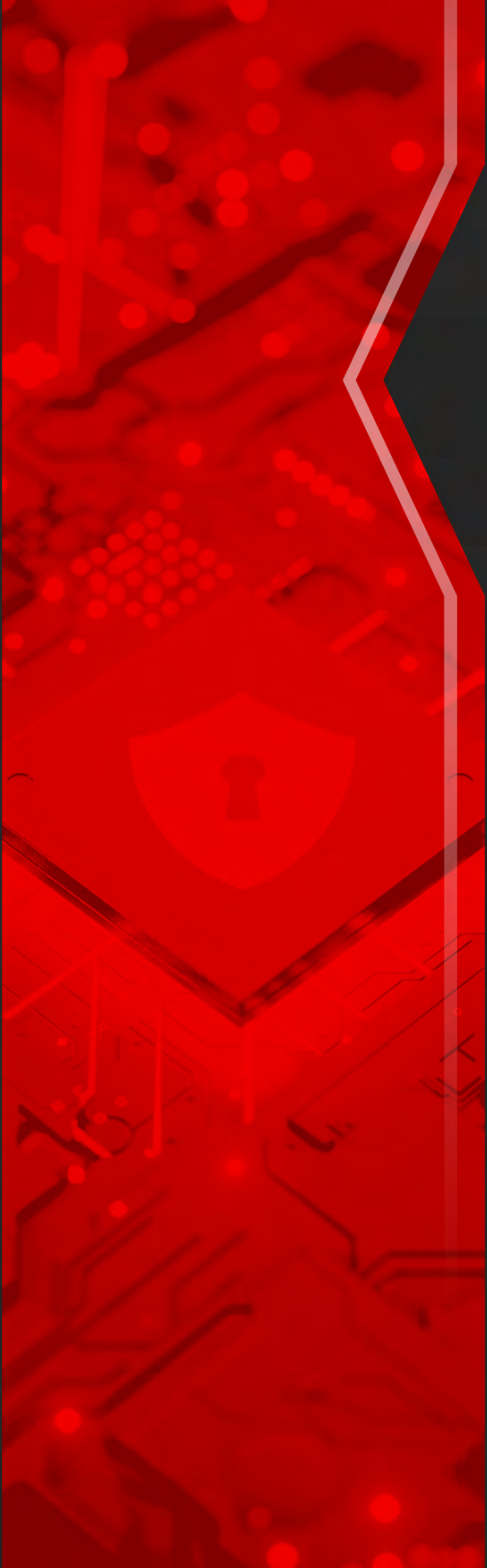


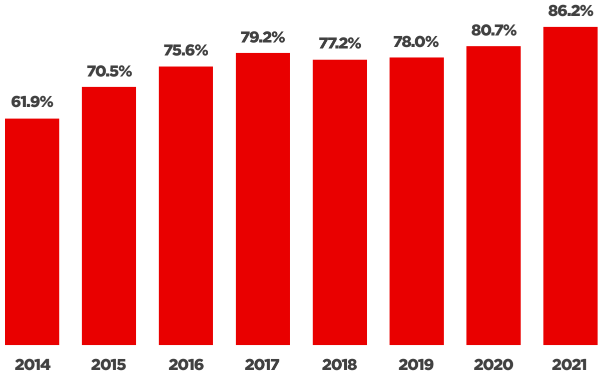
STATE OF THE UNION

COLTON COMPUTER TECHNOLOGIES

CYBER REPORT
JULY 2022

Colton Computer Technologies
coltoncomputers.com.au

Cyber security threats have increased year on year since their inception.



Above: Percentage of organisations compromised by at least one successful attack.

So, why should you care?

75% of all cyber attacks now target small businesses with less than 20 staff.

87% SMEs believe their business is safe from cyber attacks because they use anti-virus software alone.

60% of small businesses impacted will go out of business within 6 months.

The 2022 Cyber Security Landscape

- With each new technology comes new threats, meaning cybersecurity needs to be a continual focus for your business.
- Ransomware is one of the biggest threats in Australia, with a 15% increase in reported attacks in 2021.
- Supply chain attacks, where cybercriminals deliver viruses or other malicious software via a vendor or supplier to gain access to sensitive company information.
- Anti-virus software isn’t enough – cyber criminals attack this first. Continual protection and detection are essential.
- The rise in remote working means attack surface expansion and vulnerable endpoints. In plain English - there are more entrances for cybercriminals to get in and your company generally has less control over the security of the networks and devices.
- Multi-factor authentication will become the norm.
- Cybersecurity insurance premiums are rising along with the need to invest in it. As of 2019, only 27% of Australian SMBs had cybersecurity insurance.

Corporate Risk Management

Many smaller organisations might still be wrapping their heads around what risk management is all about, how they should be assessing risks and what plans they should have in place to mitigate these risks. We recommend that the first port of call is establishing a business continuity plan.

In simple terms, business continuity is your ability to keep doing business if something goes wrong, like a fire, flood, internet outage, data breach, cash flow shortage or unexpected pandemic. Every business, regardless of size, should have a business continuity plan to help you understand the risks and make your organisation as resilient and adaptable as possible.

Need some business continuity support?

Check out the resources on our website: **https://coltoncomputers.com.au/business-continuity-2021/**

Cyber Insurance Industry Changes

According to the Insurance Council of Australia, only about 20% of SMEs and 35-70% of larger businesses have standalone cyber insurance. CGU states that organisations with up to 250 employees are the most at risk from cyber incidents. We can assume that bigger organisations have cyber security specialists, making it 'harder' for cybercriminals. The oft-used phrase 'path of least resistance' springs to mind in this instance. Basically, you want to make it as hard as possible for the cyber criminals within your budget.

The unexpected benefit of investigating cyber insurance is that because there isn't a claim history to estimate cover or policy types, the insurer takes a risk audit of your systems and infrastructure. This will help you identify your weaknesses within the organisation and take steps to remediate and better protect your organisation.

The cyber insurance industry is experiencing rapid change. Cyber-related losses continue to rise in both frequency and severity. Insurers continually monitor and adjust their risk appetite and capacity, together with coverage, limits, and pricing, both in Australia and globally. The rise in government regulations and financial penalties mean that cyber insurance is constantly restructuring their coverage because the loss severity has caught them out.

In 2021, Marsh stated that cyber insurance premiums had risen by up to 80% and that claims were up by 50%. And that's not limited to one particular sector or vertical. They were at pains to call out that whilst the ransomware gets the news headlines; it's the remediation costs that are just as significant.

Despite the rise in premiums and decrease in policy coverage value, Marsh saw a 23% increase in organisations buying cyber insurance.

H1 Australian Cyber Market Snapshot

23%
Organisations purchasing cyber insurance.

20-80%
Premium increase.

50%
Frequency of claims.

Source: Marsh, Mid-year Insurance Market Update, 2021, 8.

Maximising tax benefits + small business tax incentives

In FY22, SMB owners were eligible for up to $1 billion in tax breaks for digital spending, including upgrades to cybersecurity systems. This incentive was part of a government push for more firms to embrace the online economy by actively supporting businesses to improve digital security. The government allowed eligible businesses to deduct $120 for each $100 put towards services to support their digital capacity. These tax incentives included:

✓ **Managed Services** ✓ **Cyber security training** ✓ **Cyber security systems** ✓ **Cyber security insurance**

While there hasn't been an FY23 announcement yet, keep your eye out for similar tax incentives this financial year. With cyber as a crucial business priority, every company should take advantage of the tax breaks to ensure they are better covered.

Business leadership challenges

In May, we saw **the first fine from ASIC** in response to the Notifiable Data Breach laws. This was issued in response to multiple breaches that occurred from June 2014 until May 2020. The findings were that this organisation;

Failed to have adequate risk management systems

Failed to have documentation and controls in respect of cybersecurity and cyber resilience.

Failed to remediate to an appropriate level following the incidents

As a result, the organisation has been fined $750,000.

This incident highlights the financial penalties that apply to Australian businesses for data breaches, which are incremental to the operational costs at the time of the breach and any reputational damage.

According to the OAIC report for July-December 2021, 41% of breaches resulted from human error. This statistic highlights the need for employee training and constant review of skills relating to cyber security. After all, we're all infallible, but keeping the right behaviours top of mind can reduce this risk.

Whilst it pains us to mention it, the pandemic has changed what the network perimeter looks like. Employees will continue to work in a hybrid model and potentially rove coffee shops and unsecured wifi networks for years to come. Educating staff on best practices about accessing these networks and what they should and shouldn't access whilst they're on an unverified network are now conversations that need to be part of the onboarding process.

Reputational risk and client trust are now becoming business priorities when making decisions relating to cyber security because it's not a case of if but when. Which is why it is crucial to ensure you've got a rapid response plan and communication clearly defined and ready when you need it.

So what should you be doing?

Checklist

- Prepare a data breach response plan
- Conduct quarterly comprehensive cybersecurity training for staff
- Use Multi-Factor Authentication and control access
- Check your email security regularly using ACSC’s handy step-by-step guides for Outlook and Gmail
- Make sure that you have up-to-date cyber insurance
- Consider an investment in cyber security to take advantage of the tax incentives

If you need help or simply just want to chat to us about any of the points raised in this document, reach out to the Colton team at any time on 02 6361 1116 or sales@colton.com.au.