CYBER 101:
THE INSIDE SCOOP

COLTON COMPUTER TECHNOLOGIES

CYBER REPORT
NOVEMBER 2022

Colton Computer Technologies
coltoncomputers.com.au

“ Prevention is critical to conserve scarce resources so that they are available to focus on the larger, more devastating attacks that require a human response.

Better protection helps burn down the haystack, revealing the needles that need extra attention. ”

Joe Levy
Sophos CTO

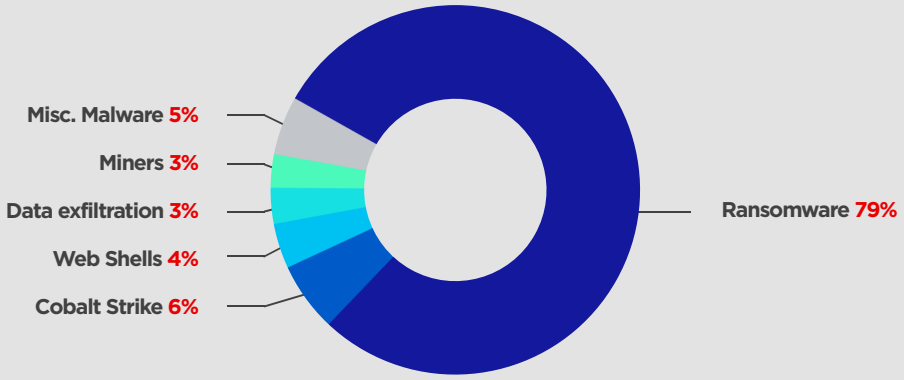
The current cyber landscape

In 2021, there was an increase of nearly **13% in the number of cyber-attacks in Australia.** And unfortunately, around 43% of these attacks **target SME businesses.** As well as being at high risk of attack, small to medium businesses can find it harder to recover from a cyber breach, which could result in the following:

- **Data loss**
- **Financial damage**
- **Damage to reputation**
- **Exposure of their sensitive business data**
- **Unauthorised control of physical environments**
- **Malware attacks or viruses**

Ransomware continues to be the leading form of attack. In 2020-2021, 79% of the incidents that Sophos's rapid attack response responded to were ransomware attacks.

Sophos Rapid Response, reason for incident response engagements 2020-2021



SOPHOS

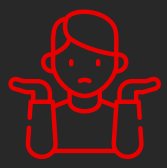
Fig 1. While ransomware attack response accounted for most of the incidents the Sophos Rapid Response team was involved in during the past year, it didn't account for them all. Removal of Cobalt Strike Beacons, cryptominers, and even web shells also prompted extra attention, especially in the days following the revelations of the Proxylogon, and later Proxyshell, exploits, which resulted in a lot of people quickly becoming familiar with how dangerous a web shell could be.

Earlier this year, the Australian Cyber Security Centre (ACSC) released a statement encouraging Australian organisations **to urgently adopt an enhanced security posture** in light of the heightened threat environment. While the warning was linked to Russia's attack on Ukraine, it echoes the ongoing message from the ACSC and other cyber organisations.

Considering the rise in cyber-attacks, it is alarming that Australian business owners are underprepared to deal with these incidents.

49% of SMEs have experienced a cyber-attack in the last 12 months

66% of small businesses are not protecting their website.



85% don't know how to handle an attack.

Cyber-attacks are becoming more challenging to deflect

Even companies investing in a cybersecurity strategy are finding it harder to halt the attacks. As technology evolves, cybercriminals adapt quickly to become more targeted, quicker to respond to vulnerabilities and increasingly savvy in their approaches. Let's take a look at two significant challenges for technology leaders.

1. The increasing threat surfaces

There are four primary reasons that cybersecurity threat surfaces are increasing. The first is the rapid adoption of the cloud. While the cloud itself isn't inherently insecure, outsourcing your data storage to a third party can lead to confusion around who is responsible for which aspect of data privacy and security. The second contributor is the increase in digital transformation – the more organisations switch to online business, the greater their exposure to potential cyber risks.

And the third factor is remote work. With hybrid working models and working from home here to stay following COVID-19, companies are struggling to maintain a consistent level of security in the home office. Connections to the company network are less secure, collaboration tools often have a minimum of security in their default setting, and less connected employees are more likely to click on dodgy phishing emails as they aren't in the loop.

2. The growing sophistication of the attacks.

Cybercriminals are adapting to move swiftly and leverage operational opportunities and world events to deploy targeted ransomware. In simple terms, they are taking advantage of significant incidents such as the pandemic and Russia's attack on Ukraine to target vulnerable people who may be panicking and less likely to cross-check standard cyber safety markers.

We are also seeing a rise in disruptive operations, where attackers use ransomware to encrypt target networks. They then leak victim information through social media, chat platforms and dedicated leak sites to amplify the impact of the data breach.

Why cyber insurance is crucial for businesses of all sizes

This challenging landscape makes it essential that companies protect their data from potential attacks that could cost them thousands of dollars, impact their reputation and close their business. But having cyber security measures like multi-factor authentication, access control, and encryption is not enough.

20% of SMEs have standalone cyber insurance

35-70% of larger businesses have standalone cyber insurance

A cyber insurance policy is designed to protect businesses from the impact of internet-based threats that may affect their IT infrastructure and data. Since **60% of small businesses impacted by a cyber-attack will go out of business within six months,** this protection is crucial.

It can cover costs to your business, including:

- **Liabilities relating to breach of privacy law**
- **Network security failures such as ransomware, extortion demands, data breaches, business email compromises and malware infections**
- **Performance failures or errors that prevent you from fulfilling your customer agreements**
- **Media liabilities relating to intellectual property and patent infringement**
- **Network business interruption coverage including fixed expenses, lost profits, and extra costs**

Due to the high number of claims in recent years, the cyber insurance industry is introducing tighter controls around the security measures you need in place to qualify. So, just like your home insurer wants to know whether you have deadlocks on your doors and locks on your windows, your cyber insurer wants to see that you are taking the required steps to protect your organisation's data.

What you need to do

So, what cyber protection and controls do you need to qualify for cyber insurance? We have compiled a comprehensive checklist to ensure that you can get the cover you need while knowing that you are putting the appropriate protective measures in place.

- **Revenue**
  - ☐ Annual revenue
  - ☐ Revenue by state or territory

- **Details of previous cyber incidents**
  - ☐ Description and date of incidents
  - ☐ Financial impact
  - ☐ Mitigating steps to avoid future incidents
  - ☐ Any current risk factors that could give rise to a Data Breach or Cyber incident

- **IT infrastructure and resourcing including:**
  - Managed service provider
  - Number of servers on your network
  - Number of desktops and laptops
  - Annual IT budget
  - Percentage spent on IT security
  - Any third-party technology partners for IT Infrastructure

- **Data storage and management**
  - Data types
  - Data protection measures (access controls, encryption, network segmentation etc.)
  - Deletion of old records
  - Storage, frequency and testing of backups
  - Number of backup copies and how you prevent multiple copies from being impacted by the same event
  - Recovery time

- **Endpoint security**
  - The Endpoint Protection and Endpoint Detection and Response you use on your network
  - How these products are monitored and managed
  - Whether they cover all endpoints on your network

- **Perimeter security**
  - Next-generation firewalls in use
  - Regularity of vulnerability scanning of network perimeter
  - Frequency of penetration testing of network architecture and whether a third party conducts this
  - Multi-factor authentication for remote access to your network
  - Methods to secure remote access to your network

- **Email security**
  - Multi-factor authentication for remote access to company email accounts
  - Use of emailing filtering software

- **Network security**
  - How you protect privileged user accounts
  - Whether non-IT users have local administrator rights on their computer
  - Use of a network monitoring solution to alert you to malicious/suspicious behaviour
  - Use of a Security Operations Centre (SOC)
  - Whether you have any end-of-life or end-of-support software
  - Patch management process to ensure critical patches are applied in a timely process
  - Significant changes planned for your IT infrastructure

- **Staff training**
  - Phishing testing
  - Responsible password practices
  - Cyber best practices
  - Cyber incident response preparedness
- **Additional controls that you use**
- **Audit information**
- **Procedures around intellectual property**
- **Legal counsel relating to privacy policy, terms of use, terms of service and customer policies**

Proposed Legislation

Under a new bill put forward by the Albanese Government, the maximum penalty for serious or repeated privacy breaches will increase from $2.22 million to whichever is the greater sum, either:

- $50 million
- Three times the value of any benefit obtained through the misuse of information
- 30 per cent of a company's adjusted turnover in the relevant period

The Privacy Legislation Amendment (Enforcement and Other Measures) Bill 2022 will also strengthen the Notifiable Data Breaches scheme, give the Australian Information Commissioner greater power to resolve any privacy breaches, and provide the Australian Communications and Media Authority with increased information sharing powers. The proposed amendment, along with new cyber governance principles for boards and directors that have been released by the Cyber Security Cooperative Research Centre (CSCRC) and the Australian Institute of Company Directors (AICD), places clear responsibility on each company to take proactive measures.

If you are concerned about your organisation's cyber resilience, get in touch with the Colton team for a check up.

02 6361 1116
sales@colton.com.au
156 Moulder St, Orange NSW 2800