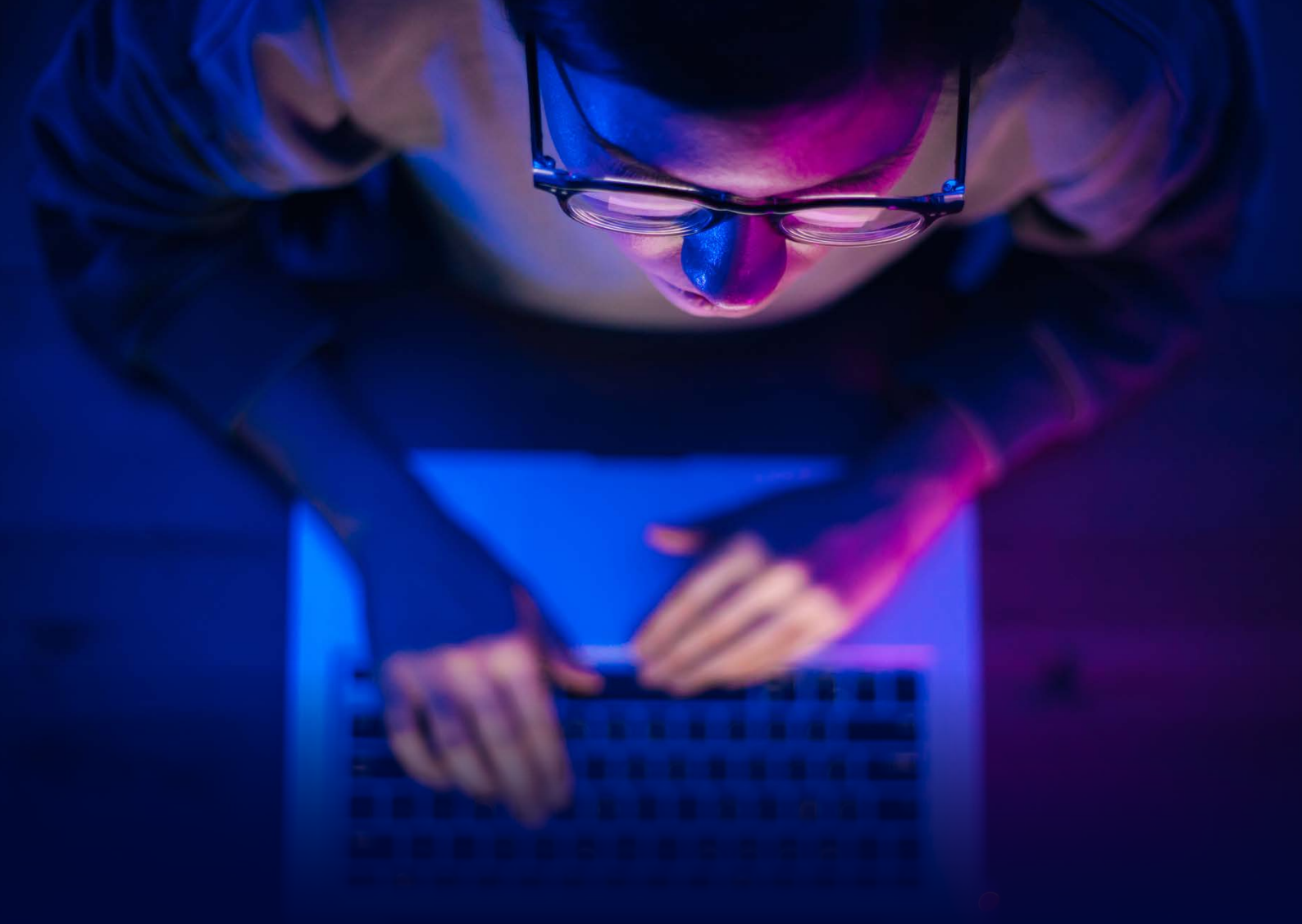
technologyone

Transforming business, making life simple

Ransomware Basics

Contents.



What is a ransom attack?

There are numerous types of ransom attacks. Two of the main types are:

Ransomware: when malicious software (malware) encrypts data and demand for a ransom is made in exchange for decryption.

Cyber thieves: find an exploit to steal a copy of your data to coerce payment of a ransom by threatening to publicly leak or sell your data or authentication information.

How does a ransom attack work?

Several social engineering methods are used to infect or exploit a vulnerability on a computer or system. Some examples are:

Email phishing: messages that include either a malicious attachment or a link to a compromised website. Once the user opens the attachment or clicks the link, the ransomware can infect the victim's computer and spread throughout the network.

Scareware: uses popups to convince victims they have a virus and directs them to download fake software to fix the issue.

Malvertising (malicious advertising): injects malicious code within digital ads.

Once ransomware infects the system, it allows the threat actor to block access to the storage device or encrypt some or all of the files on the device or send the files to the threat actors computer.

While you may be able to remove the malware and restore the system files will remain encrypted because they've already been made unreadable.

Decryption is impossible without the attacker's key. Such malware may lay dormant for long periods of time.

Ransom attacks in Australia

The rate of ransom attacks in Australia is above global average and all the trends are upwards. Consistent with global trends, cybercriminals are successfully using ransom attacks to disrupt operations and cause reputational damage to Australian organisations.

Most ransom attacks occur after other malicious activity has been conducted against an organisation (e.g. phishing campaigns).

Ransom attacks will remain a common threat in Australia and globally due to cybercriminals' success and the industrialisation of this.

All sectors and individuals with information of value are potential targets for cybercriminals seeking opportunities for financial gain.

Australian Cyber Security Council Statistics

During the 2020-21 financial year, the ACSC observed:

Source: ACSC Annual Cyber Threat Report 1 July 2020 – 30 June 2021

67.5k
cybercrime reports

$81.45m
self-reported losses from business email compromise

$33bn
self-reported losses from cybercrime

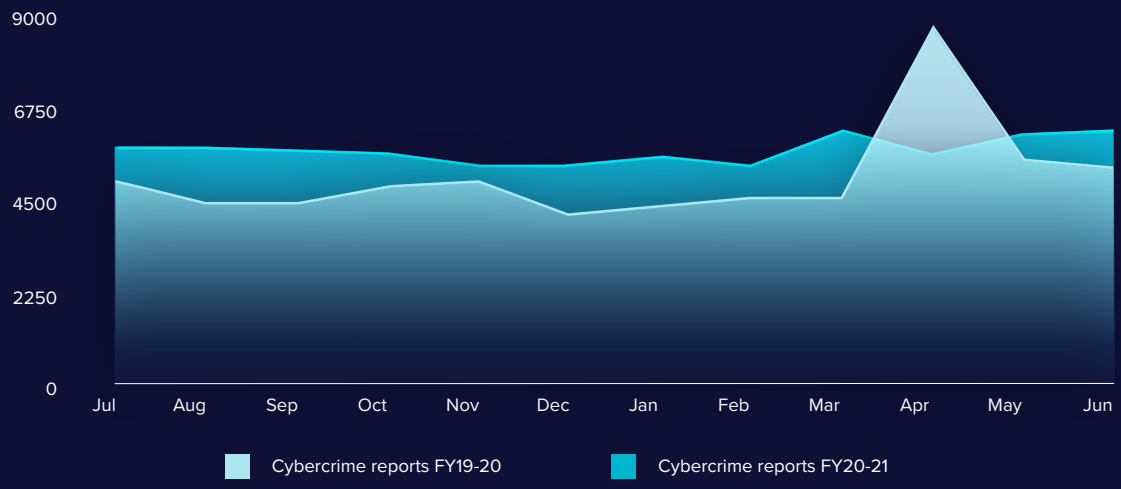
A quarter
of reported cyber security incidents affected entities associated with Australia's critical infrastructure

1.5k
cybercrime reports per month of malicious cyber activity related to coronavirus pandemic

Australian Cyber Security Council Statistics

Cybercrime reports by month for FY 2020-21 compared with FY2019-20

Source: ACSC Annual Cyber Threat Report 1 July 2020 – 30 June 2021

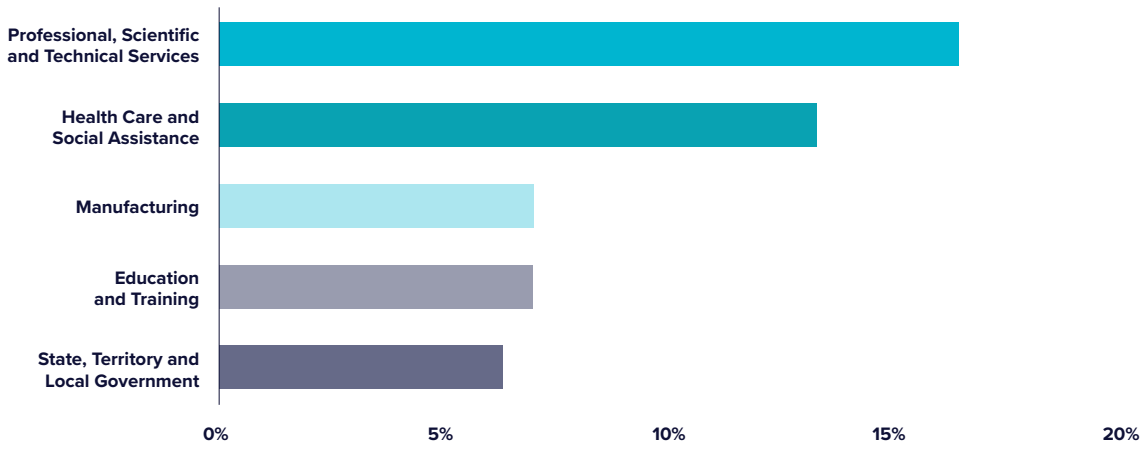


Note: The notable spike in April 2020 relates to a bulk extortion campaign, resulting in nearly half of the cybercrime reports for that month.

Australian Cyber Security Council Statistics

Top five reporting sectors for ransomware-related cyber security incidents

Source: ACSC Annual Cyber Threat Report 1 July 2020 – 30 June 2021

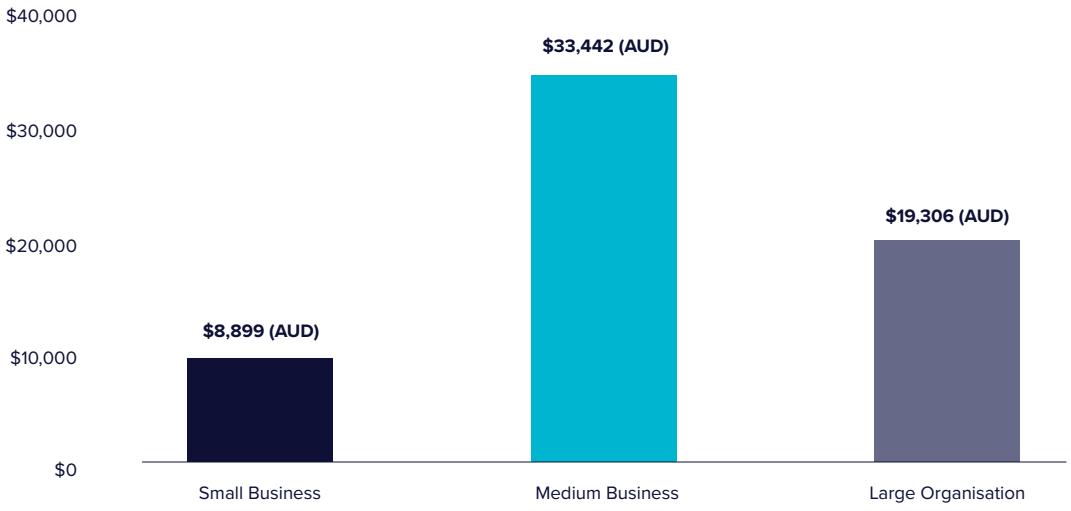


Note: While Commonwealth, state, territory, and local government accounted for approximately one third (35 per cent) of incidents in the 2020–21 financial year, the high reporting frequency of government agencies is in part due to the obligation to report significant cyber security incidents to the ACSC, and may not necessarily reflect an increased susceptibility of these networks to cyber incidents, when compared with industry.

Australian Cyber Security Council Statistics

Cybercrime reports & average reported loss by organisation size for FY2020-21

Source: ACSC Annual Cyber Threat Report 1 July 2020 – 30 June 2021

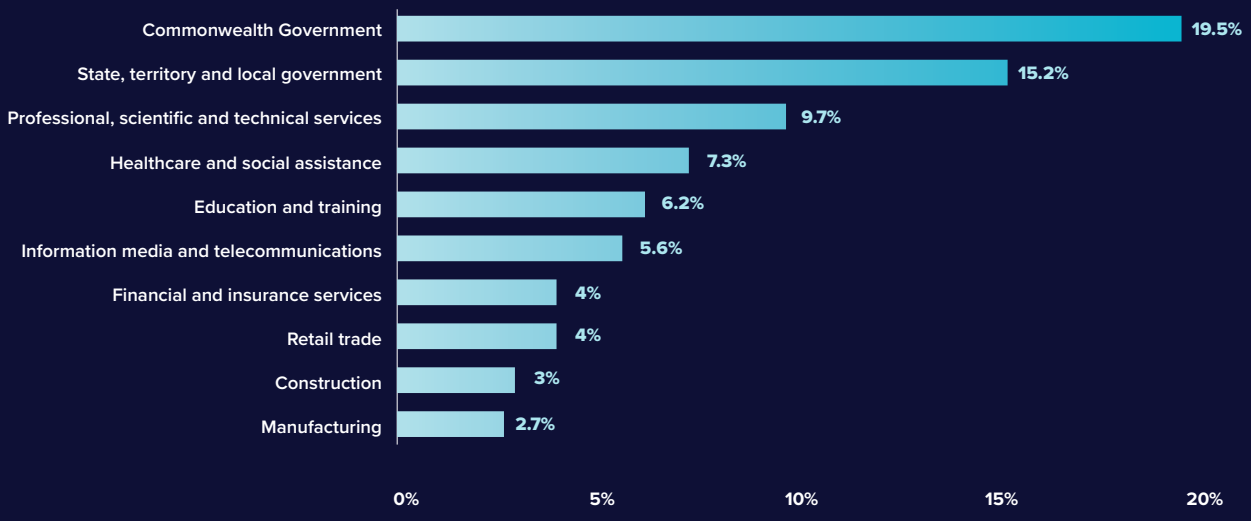


Note: Figures rounded to the nearest dollar (AUD).

Australian Cyber Security Council Statistics

Cyber security incidents by the top ten reporting sectors for FY 2020-21

Source: ACSC Annual Cyber Threat Report 1 July 2020 – 30 June 2021



Avoiding a ransom attack: preparing an effective response

Protective measures and mitigations are key to preventing ransom attacks. Adopting a 'defence-in-depth' approach, using layers of defence with several mitigations at each layer, will provide more opportunity to detect malware and stop it before it causes real harm.

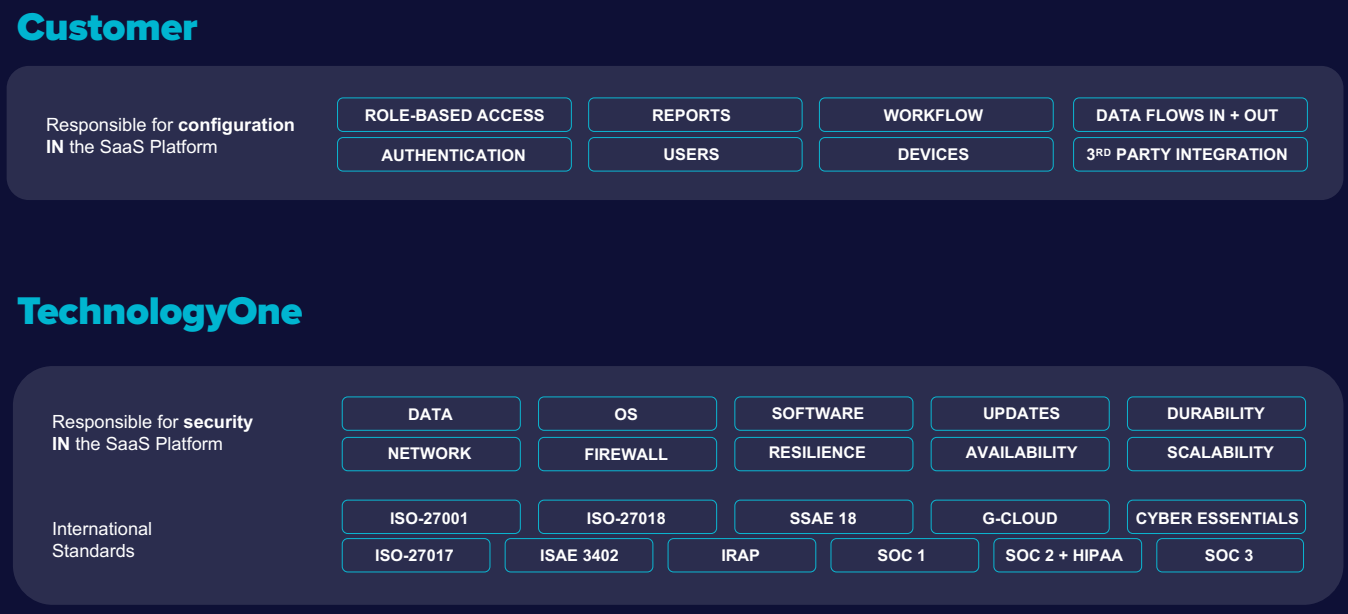
To assist with this, the ACSC has published a prioritised list called the Strategies to Mitigate Cyber Security Incidents, under which Essential Eight mitigation strategies are outlined. https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

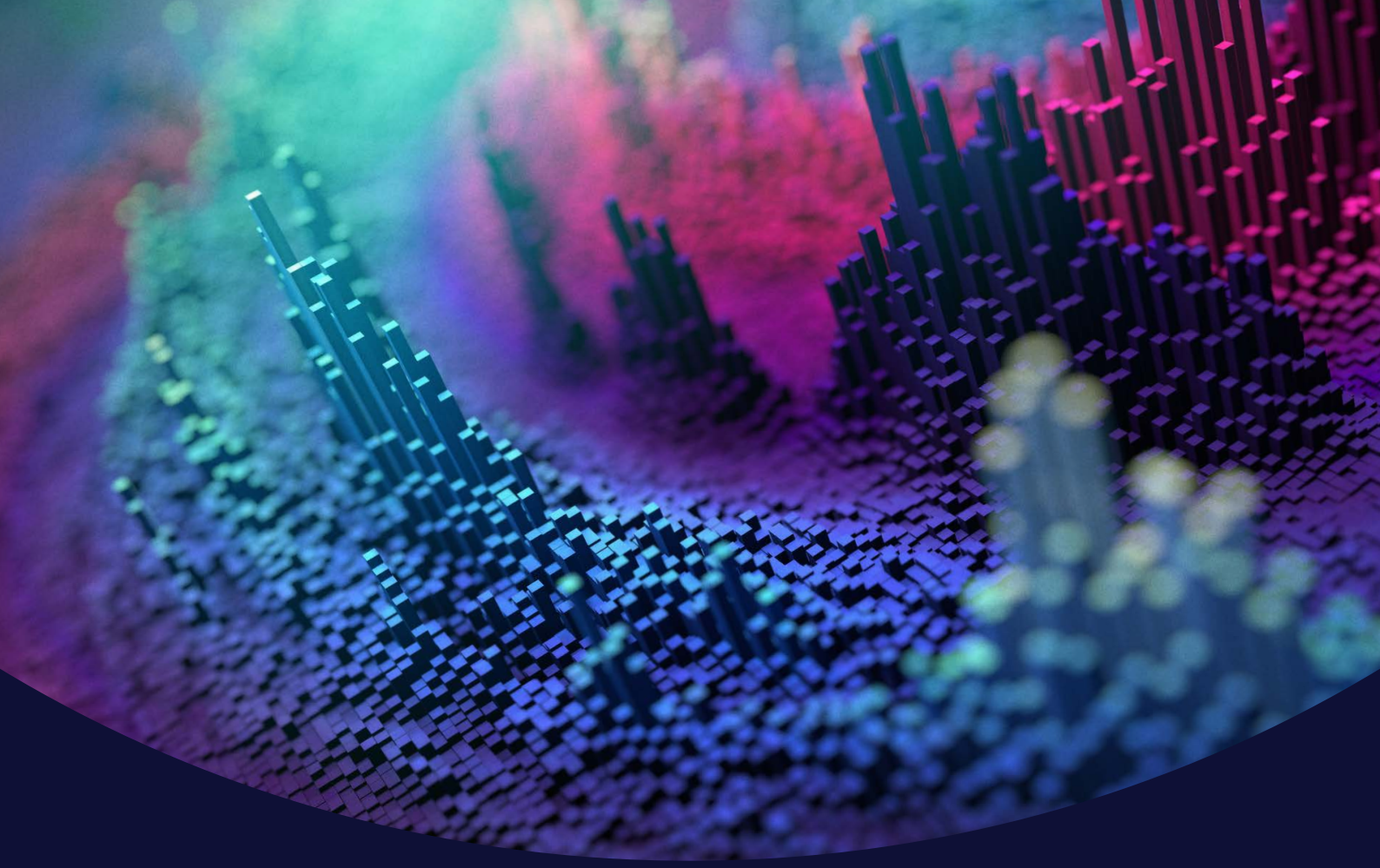
TechnologyOne's Shared Responsibility Model

TechnologyOne operate on a Shared Responsibility Model where all parties have a significant role to play in protecting the security and privacy of the system and the data contained within it. The TechnologyOne SaaS Platform integrates the latest in innovative security and privacy technologies. All SaaS customers are protected by our multi-tiered security measures and accredited procedures.

However, due to the sophisticated nature of the threats, customers are required to play their part. TechnologyOne has developed Complementary User Entity Controls (CUECs) which SaaS customers are expected to have in place for the services provided by our SaaS Platform. The controls TechnologyOne has in place are described and independently attested to in the TechnologyOne SOC Reports. These SOC reports describe the CUECs and are available to SaaS customers and their auditors along with the TechnologyOne ACSC Essential Eight Maturity Assessment letter.

For more information, please visit the Security & Trust page on our website: https://technologyonecorp.com/saas/security-and-trust





Organisations can protect themselves from ransomware using the ACSC's tailored guidance described below.

Follow the steps in the ACSC's Ransomware Prevention and Protection Guide: https://www.cyber.gov.au/sites/default/files/2020-12/ACSC_Prevention-And-Protection-Guide_1.pdf

Update devices and systems
Update software and turn on automatic operating system updates.

Enable multi-factor authentication
Have multi-factor authentication enabled by default on any corporate networks, devices or systems.

Backup data
Set up and perform regular offline backups; these are essential for recovery following a ransomware attack. Backups must be stored offline or otherwise isolated from the corporate network.

Implement access controls
Restrict administrator privileges and do not share or re-use login details.

Turn on ransomware protection
This is available on some operating systems.

Prepare a Cyber Security Emergency Plan
Prepare and regularly exercise this plan to ensure everyone is familiar with the processes and understands their roles.

Reality Check

- You don't need to be a technical expert to make informed cyber security decisions
- A methodical approach to cyber security and enacting small changes can greatly reduce the risk to your organisation
- Cyber attacks are often opportunistic and any organisation can be impacted

Visit the Australian Cyber Security Centre website for more information: https://www.cyber.gov.au/

If you experience a ransom attack.

Advice from the Australian Cyber Security Centre

Start your own incident reponse plan:

ACSC 24/7 hotline: 1300CYBER (1300 292 371)
UK NCSC: 0300 020 0964
NZ NCSC: (04) 498-7654

Never pay a ransom
There is no guarantee hackers will restore your information, stop attacking you, or that they won't leak or sell your data. There is a risk that funds may support terrorist organisations or sanctioned entities or countries. Payment may be illegal under certain circumstances.

Seek professional help
Ransomware attacks can cause serious damage. It is hard to tackle and overcome it on your own. Find a professional to help you work through aransomware attack, and get back on your feet.

Do the following:

- Disconnect devices
- Stop the ransomware
- Run a malware scan
- Write down key details
- Get professional help
- Notify and report
- Protect from future attacks

Contact TechnologyOne

SaaS customers are required to contact TechnologyOne to report any urgent security or privacy concerns in relation to the TechnologyOne SaaS Platform.

Raise a support case
Only nominated key contacts can register an incident in the TechnologyOne Customer Community. Refer to your Customer Support Guide for more information.

1. Log into the TechnologyOne Customer Community
2. Select the 'cases' tab
3. Select 'contact support'
4. Enter the information into the required fields to register the incident.
5. Identify the case as a security/privacy issue and request a P1 rating.

Email
Email TechnologyOne to notify us of a privacy or security breach, data beach or to request data breach support/investigations.
Email **privacy@technologyonecorp.com** or **security@technologyonecorp.com**

TechnologyOne shares important and urgent security-related information with SaaS customers via the Customer Community Security Group. SaaS customers should register a nominated key representative from their organisation to receive these important security advisories. Contact TechnologyOne Support Centre and ask to be added.

Useful resources.

Australian Cyber Security Centre (ACSC)
ACSC Threat Report - 1 July 2020 to 30 June
https://www.cyber.gov.au/acsc/view-all-content/publications/acsc-annual-cyber-threat-report-2020-21

ACSC's Ransomware Prevention and Protection Guide
https://www.cyber.gov.au/ransomware/protect-yourself-against-ransomware-attacks

How to protect against Ransomware
https://www.cyber.gov.au/ransomware

Essential Eight Explained
https://www.cyber.gov.au/acsc/view-all-content/publications/essential-eight-explained

Report a cyber security incident
https://www.cyber.gov.au/acsc/report

Strategies to mitigate cyber security incidents
https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents

Quick wins for your website
https://www.cyber.gov.au/acsc/view-all-content/publications/quick-wins-your-website

Multi-factor authentication
https://www.cyber.gov.au/acsc/view-all-content/advice/multi-factor-authentication

Software updates
https://www.cyber.gov.au/acsc/view-all-content/advice/multi-factor-authentication

Register for ACSC Alert Service
https://www.cyber.gov.au/acsc/register/individuals-and-families

COVID-19 malicious scams – threat awareness and guidance
https://www.cyber.gov.au/acsc/view-all-content/advisories/covid-19-malicious-scams-threat-awareness-and-guidance

National Cyber Security Centre (NCSC) NZ
Ransomware guidance and resources:
https://www.ncsc.govt.nz/newsroom/ransomware-advice/

Report a cyber security incident (CERT NZ) https://www.cert.govt.nz/individuals/common-threats/ransomware/

National Cyber Security Centre (NCSC) UK
Mitigating malware and ransomware attacks
https://www.ncsc.gov.uk/guidance/mitigating-malware-and-ransomware-attacks

Guidance on how organisations can protect themselves in cyberspace https://www.ncsc.gov.uk/collection/10-steps

Resources designed to encourage essential cyber security discussions between the Board and their technical experts
https://www.ncsc.gov.uk/section/board-toolkit/home

Technical advice via infographics
https://www.ncsc.gov.uk/information/infographics-ncsc

Cybersecurity and Infrastructure Security Agency (CISA) US
Ransomware guidance and resources
https://www.cisa.gov/ransomware

Ransomware guide
https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf

TechnologyOne
Security & Trust page
https://technologyonecorp.com/saas/security-and-trust

Register for Security Advisories
https://go.technologyonecorp.com/n0Du0hq03rYL0GM0fo006E0

About TechnologyOne.

TechnologyOne (ASX: TNE) is Australia's largest enterprise software company and one of Australia's top 150 ASX-listed companies, with locations across six countries. We provide a global SaaS ERP solution that transforms business and makes life simple for our customers. Our deeply integrated enterprise SaaS solution is available on any device, anywhere and any time and is incredibly easy to use.

Over 1,200 leading corporations, government agencies, local councils and universities are powered by our software. For more than 34 years, we have been providing our customers enterprise software that evolves and adapts to new and emerging technologies, allowing them to focus on their business and not technology.

ACN 010 487 18

Ready to learn more?
technologyonecorp.com

technologyone
Transforming business, making life simple