REUTERS
World
Business
Legal
Markets
Technology
2 minute read · October 5, 2022 7:53 AM GMT+11 · Last Updated 5 months ago
Australia's Telstra hit by data breach, two weeks after attack on Optus
By Byron Kaye
Australian Government
Australian Signals Directorate
ACSC Australian Cyber Security Centre
Report
Search
Contact us
Individuals & Families
Small & Medium Businesses
Organisations & Critical Infrastructure
Government
Learn
Medibank Private Cyber Security Incident
Content complexity
Simple
Home > About the ACSC > View all content > View all alerts > Medibank Private Cyber Security Incident
Content written for
Individuals & fa
Small & medium businesses
Cyber Security Centre is working closely with Medibank
recent incident.
BBC
Sign in
NEWS
Home
War in Ukraine
World
Africa
Australia
Optus: How a massive data breach has exposed Australia
29 September 2022
yes
OPTUS
Australia's Data Breaches Continue With
The Guardian
Opinion
Sport
Culture
Project Syndicate
Retail
This article is more than 2 months old
Telstra sorry for publishing up to 30,000 customers' details online
Follow our Australia news live blog for the latest updates
Get our morning and afternoon news emails, free app or daily news podcast
Medibank
This article is more than 2 months old
Medibank hackers announce 'case closed' and dump huge data file on dark web
Medibank confirms it may be the full trove of hundreds of thousands of customers' private records that were stolen from the health insurer
Follow our Australia news live blog for the latest updates
Get our morning and afternoon news emails, free app or daily news podcast
Paid content
The road to the future: how tech is changing our everyday lives
medibank

# IT Security Checklist for 2023: STRENGTHEN YOUR CYBERSECURITY

**OPTIMISE** YOUR OPERATIONS

Canon CANON BUSINESS SERVICES **ANZ**

# IT Security Checklist for 2023: STRENGTHEN YOUR CYBERSECURITY

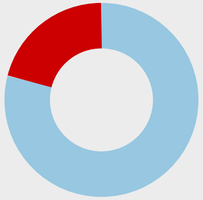
## In 2023, no company can truly say that they aren't at risk of an attack. Given the way cybersecurity threats have evolved, SME targets can be just as appealing as enterprise organisations – in fact, they represent a growing number of data breach reports.

The Australian Cyber Security Centre (ACSC) Small Business Survey, for example, reports that "62 per cent of respondents have experienced a cyber security incident", even though almost half of participants reported spending "less than $500 on cyber security per year".

To assess how your current security posture stacks up – and to avoid becoming this year's big news headline – use our IT security checklist to strengthen your systems as we continue into 2023. Not only can taking these steps reduce your risk, but doing so may also help you to reduce your cybersecurity insurance premiums, if you've seen the cost of your cover soar recently.

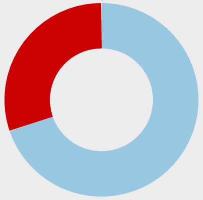
Of course, some of these items may not apply to you, depending on your organisation's type, size, geographic region, or industry. If you need help assessing your company's specific vulnerabilities, reach out to Canon Business Services (CBS) for help with a customised security assessment.

**TALK TO ONE OF OUR EXPERTS TODAY**



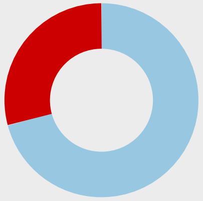
**20%**

of organisations **lose customers** during an attack



**30%**

of organisations **lose revenue** during an attack



**28%**

of attacks **come from the inside** – harder to detect

# FOUR KEY AREAS

## Document your environment

Why it's important to begin by assessing your environment and documenting all the key elements.

## Manage your technology

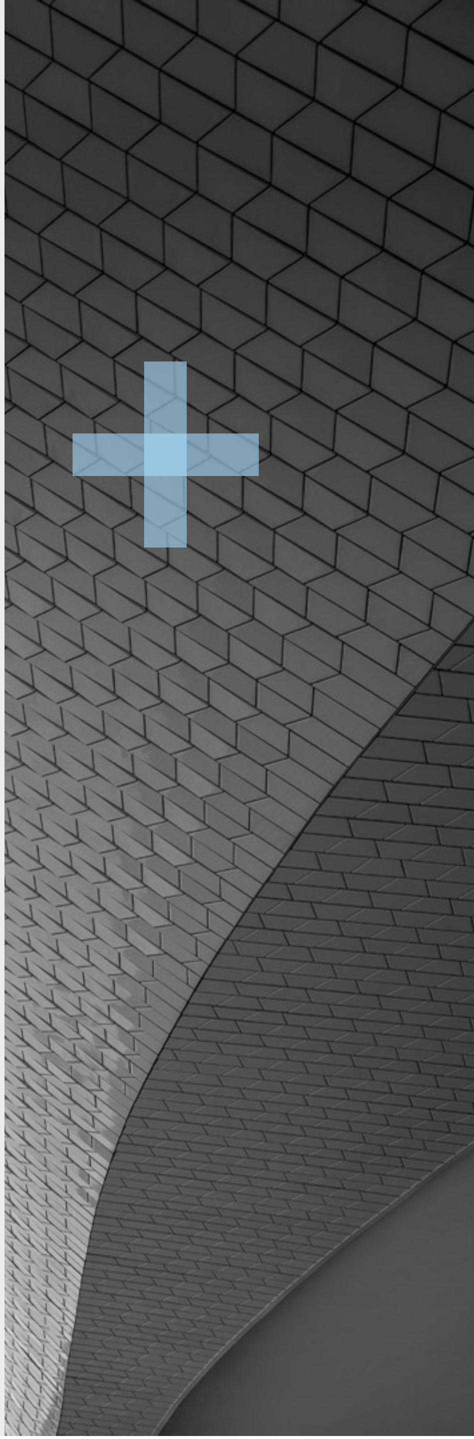
When it comes to managing the security of your technology, make sure you can tick each of the boxes. If you can't, take action to do so ASAP, either on your own or with the support of an external partner.

## Manage your people

In addition to securing your technology, invest in educating all of your company's users on proper security behaviours.

## Monitor your progress

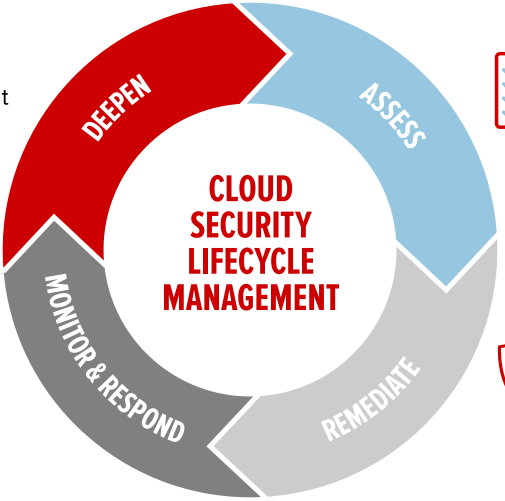
To maintain protection once you've established practices that govern the security of your technology and people, establish ongoing processes that tick each of the boxes.



# HOW TO USE THE CHECKLIST

This is our 2023 Cybersecurity checklist. It will help you to review existing security measures, assess your current posture and reduce your risk. Tick all the checkboxes that apply to your business's current operational environment. If you find the security measures to be insufficient, talk to one of our experts about how we can help.

1. Click all the boxes that apply to you in each section
   ✓ **Tick all that apply**
2. Each box you click will show a tick
3. Any that remain unticked will highlight how your security stacks up against what we offer, and what steps you can take to review and update them within your business
4. Additionally, you can watch our webinar walkthrough on how to use this checklist. ▷

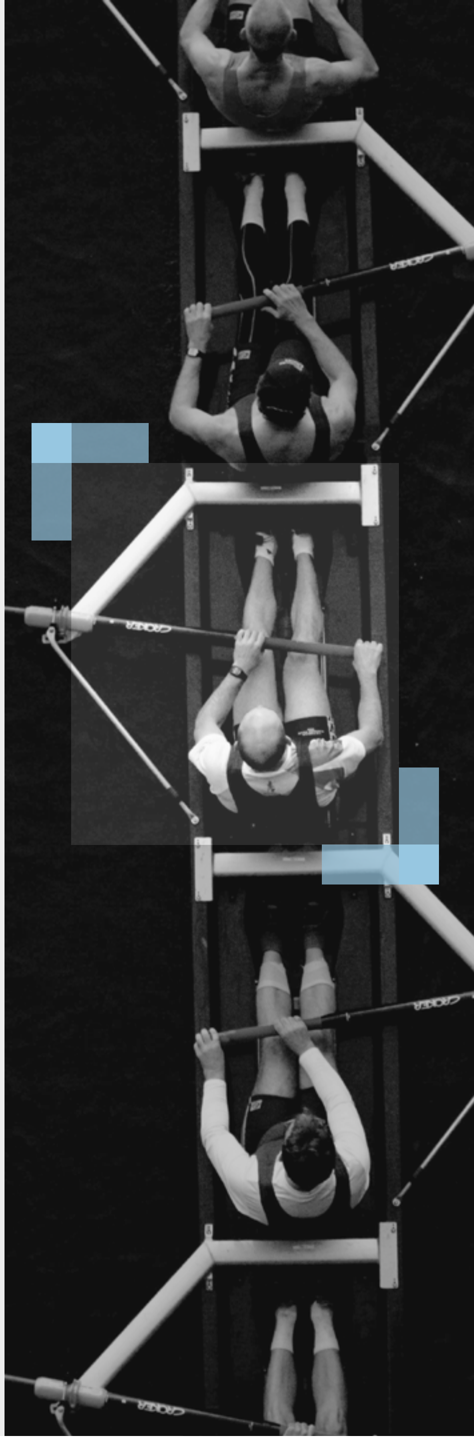


**DEEPEN**
- Continuos improvement
- Raise security maturity

**ASSESS**
- Azure config and security assessment
- Full cloud and hybrid cloud security assessment
- Penetration testing

**MONITOR & RESPOND**
- Cloud security managed services implementation
- 24/7 security monitoring with Azure Sentinel

**REMEDIATE**
- Security uplift
- Cloud security uplift to full featured M365 E5
- Implementation of Azure Sentinel



# YOUR 2023 CYBERSECURITY CHECKLIST STARTS HERE

## Document your environment

✓ **Tick all that apply**

To build a strong security program, you need to understand the environment you're working in. That's why it's important to begin by assessing your environment and documenting all of the following assets or elements:

□ Employees (including any established privilege levels)

□ Contractors

□ External or guest users

□ Networks

□ Endpoint devices (including desktop computers, mobile devices, routers, etc.)

□ Servers

□ Applications

□ Software programs and licenses

□ Data types and storage locations (especially sensitive or PII data)

□ Physical locations, including remote work locations

**Depending on the specifics of your situation, it may also be a good idea to:**

□ Document how these different assets and elements interact with each other

□ Identify potential weaknesses in asset interactions that allow users greater access than is required

□ Establish a process for regularly updating your documentation

□ Assign responsibility for keeping this documentation updated to a person, role, or department

TALK TO ONE OF OUR EXPERTS TODAY

## Manage your technology

**✓ Tick all that apply**

Next, when it comes to managing the security of your technology, make sure you can tick each of the following boxes. If you can't, take action to do so ASAP, either on your own or with the support of an external partner.

- □ Our data is regularly backed up
- □ Our backups are disconnected from our network to ensure data can be restored easily
- □ Where appropriate, our data is properly encrypted and stored securely
- □ We have a defined process for deleting data from all locations, when appropriate
- □ Our devices and applications are kept up-to-date, and new versions or patches are implemented automatically or in a timely manner
- □ We have turned on multi-factor authentication, where appropriate
- □ We use privileged access management, role-based access control, and/or conditional access to limit unnecessary access, where appropriate
- □ We have secured and/or segmented our network to minimise potential intrusion and lateral movement

**TALK TO ONE OF OUR EXPERTS TODAY**

## Manage your technology – continued

✓ **Tick all that apply**

□ We use firewalls and endpoint-monitoring applications to protect our devices, where appropriate

□ We have established – and enforce – appropriate ‘bring your own device’ (BYOD) policies that protect our networks and data

□ We use a ‘Zero Trust’ or ‘need-to-use’ basis when assigning user access privileges

□ We have technology in place to scan incoming emails for potential threats

□ We regularly identify and replace legacy technology that can no longer be properly secured

□ We have identified and addressed any potential security risks associated with the use of third-party systems or technology

□ We have technology that provides end-to-end visibility across networks, applications, users, and data

□ We have the technology to identify anomalies, generate necessary alerts, and take the necessary actions to prevent breaches.

TALK TO ONE OF OUR EXPERTS TODAY

# IT Security Checklist for 2023: STRENGTHEN YOUR CYBERSECURITY

## Manage your people

✓ **Tick all that apply**

Truly, your systems are only as secure as the people working within them. In addition to securing your technology, invest in educating all of your company's users on proper security behaviours. Can you tick each of the following boxes?

- □ We regularly train our team on safe cybersecurity behaviours (at least every 3-6 months)
- □ We require the usage and regular updating of secure passwords
- □ We limit the use of shared accounts among users
- □ We have an established process for onboarding new users in a secure fashion
- □ We have an established process for revoking access from terminated users upon (or prior to) their exit
- □ We have educated our board members on their security responsibilities and report to them regularly
- □ We regularly check employee email addresses for evidence that they've been involved in known breaches
- □ We understand who within our organisation is handling our sensitive data and have trained them on appropriate practices

**TALK TO ONE OF OUR EXPERTS TODAY**

## Monitor your progress

✓ **Tick all that apply**

Finally, keep in mind that security is not a 'one-and-done' activity. To maintain protection once you've established practices that govern the security of your technology and people, establish ongoing processes that tick each of the following boxes:

□ Someone in our organisation is responsible for staying up-to-date on new cybersecurity threats

□ We regularly evaluate the appropriateness of external partnerships, such as those with IT managed services (MSPs), managed security service providers (MSSPs), or SIEM service providers.

□ We regularly evaluate our security preparedness to identify and prioritise specific risks for remediation

□ We conduct penetration testing, as appropriate, to assess our cyber defences

□ We have a plan in place for responding to a cyberattack, should one occur

□ We have identified the resources that will support us in responding to a cyberattack, if needed

□ We understand who we need to notify in the event of a cyberattack or breach

□ We have evaluated the appropriateness of standalone cyber insurance for our organisation

□ We measure our cybersecurity posture against industry standards, frameworks, and mitigation strategies such as ISO 27001, NIST, and ACSC Essential Eight, and we stay up-to-date as IT compliance standards change

TALK TO ONE OF OUR EXPERTS TODAY

## Support for your security priorities

If our IT security checklist sounds like a lot, that's because it's meant to. Even as security management has become more complex than ever, it's become more important than ever for companies of every size.

So if you aren't sure what any of these items mean – or if you aren't sure how to implement them on your own – CBS can help. Reach out to our team for a personalised assessment of your security needs or for expert support uplifting your security in 2023.

TALK TO ONE OF OUR EXPERTS TODAY

**Canon Business Services ANZ (CBS) is proud to be among the few Australian MSSPs in the Microsoft Intelligent Security Association (MISA), which means we can better defend you against a world of increasing cyber threats. Choose the team with 3 Azure advanced security specialisations (Identity & Access Management, Cloud Security and Threat Protection) to safeguard your organisation today.**

### Disclaimer

The information contained in this e-book and checklists are for general information purposes. It does not take into consideration your business' specific needs or objectives and should not be relied upon as a basis for making any business or legal decisions. Any reliance you place on such material is strictly at your own risk. Canon Business Services recommends you speak to a professional before making any decision.

# ADDITIONAL RESOURCES

### ACSC Essential Eight Assessment

Know your organisation's cybersecurity maturity and how to optimise it.

### Why you need to start with a cybersecurity assessment

Too often, businesses focus on implementing cybersecurity measures after they've been compromised. Learn why it's important to conduct a cybersecurity assessment upfront ASAP, either on your own or with the support of an external partner.

### Funding new security requirements with no new budget

Most IT leaders are looking for opportunities to increase their security posture without requiring additional funds. Learn how you can make progress toward your ideal security posture, even with budget restrictions.

### Benefits of a Security Operations Centre (SOC)

From well known security benefits to enhanced collaboration opportunities, SOC implementation offers invaluable insight and growth potential.

### Managed Security Services: How to Choose the Right MSSP

Businesses are turning to managed IT security services providers (MSSPs) to stay secure from cyber threats. Here's how to choose the MSSP that delivers the best results for your business.

### SIEM 101: A Strategic Approach to Enhance Your Security and Compliance

Navigate our article and navigate the fundamentals of SIEM with a thorough approach for assessing your current security posture and bolstering both protection levels and compliance.

# BOOK A CONSULTATION WITH CBS

Canon Business Services offers a combination of world-class automation solutions with leading IT services to optimise business operations. We unleash our customers to focus on what sets them apart. At Canon Business Services ANZ we want to empower you to focus on the big picture – running the business. Don't let processes, capacity, and inefficiencies slow you down.

We optimise your business processes and embed enabling technologies, so you're free to focus on what sets you apart.

Work with our team to tailor a solution that tackles your greatest cybersecurity challenges with services that respond to your exact needs.

**TALK TO ONE OF OUR EXPERTS TODAY**

Canon

CANON BUSINESS SERVICES ANZ