No one does it like you

CANON **BUSINESS READINESS** INDEX

2018 Information Security Edition

EXECUTIVE SUMMARY

Australian businesses unprepared for new data laws.

The inaugural Canon Business Readiness Index on Information Security is a comprehensive study that examines the digital readiness of Australian businesses with specific reference to the new data breach notification laws coming into effect on 22 February 2018.

The study, conducted by GfK Australia in January 2018, reveals some worrying trends.

The level of concern for many businesses is too low, particularly for small businesses with 15% saying they are not at all concerned about suffering a security breach. This is a perception that is out of sync with the reality of the risk landscape.

Businesses that have completed an IT security assessment are generally more concerned than those that have not, suggesting the current lack of concern is due to a lack of awareness around the scale of the issues. Given the growing size and sophistication of security threats, businesses need to better understand the risks facing their business.

The majority of affected businesses reported not being aware of the new legislation. Of those that were aware, few scored well on 'preparedness,' despite potentially crippling fines of up to $2.1 million for non-compliance.

Businesses aren't prepared enough, particularly small businesses. Only 40% have 6 or more of the Australian Signals Directorate Essential 8 (ASD8) strategies in place, this decreases to 27% for small businesses with 12% having no ASD8 strategies in place at all.

The prognosis is clear: Australian businesses need to improve their data protection measures. Failure to do so could risk compromising confidential data, expose them to hefty fines and lead to significant reputational damage.

CONTENTS

INTERACTIVE

AUSTRALIAN BUSINESSES WORRIED ABOUT CYBER SECURITY – **IS IT ENOUGH?**

38% of Australian businesses are ‘extremely’ to ‘very concerned’ that they could suffer from a security breach within the next 12 months (with another 32% that are moderately concerned).

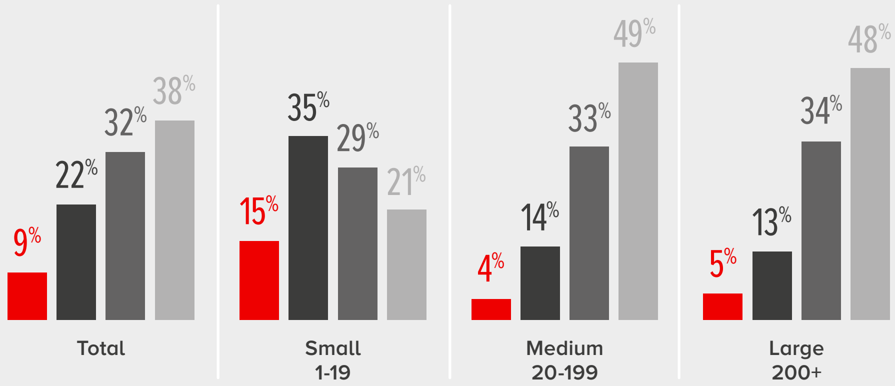
Small businesses (<20 employees) appear less concerned with only 21% extremely/very concerned and alarmingly 15% not concerned at all.

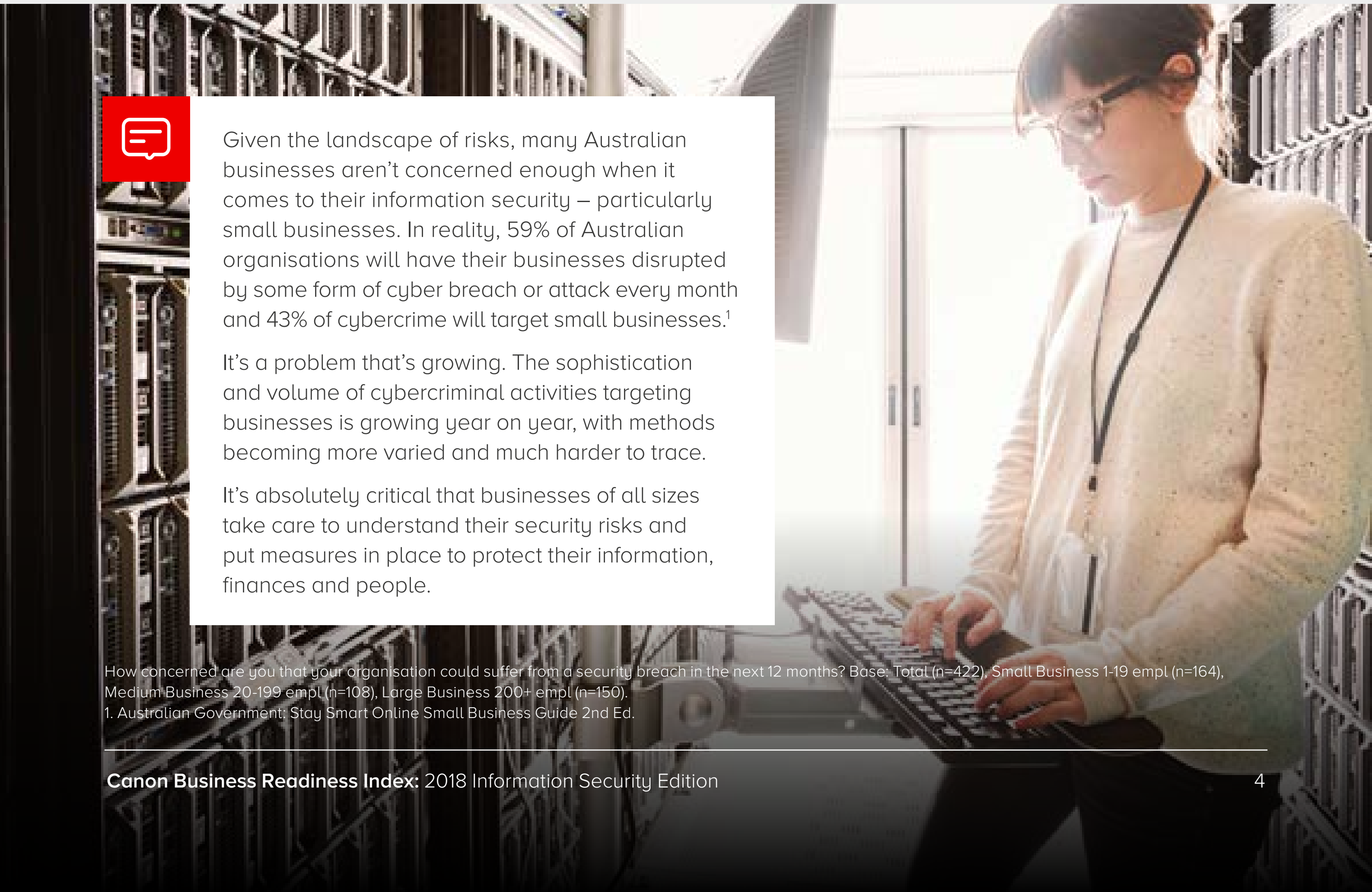
● Not at all concerned

● Slightly concerned

● Moderately concerned

● Extremely/very concerned





Given the landscape of risks, many Australian businesses aren’t concerned enough when it comes to their information security – particularly small businesses. In reality, 59% of Australian organisations will have their businesses disrupted by some form of cyber breach or attack every month and 43% of cybercrime will target small businesses.[1]

It’s a problem that’s growing. The sophistication and volume of cybercriminal activities targeting businesses is growing year on year, with methods becoming more varied and much harder to trace.

It’s absolutely critical that businesses of all sizes take care to understand their security risks and put measures in place to protect their information, finances and people.

How concerned are you that your organisation could suffer from a security breach in the next 12 months? Base: Total (n=422), Small Business 1-19 empl (n=164), Medium Business 20-199 empl (n=108), Large Business 200+ empl (n=150).

[1] Australian Government: Stay Smart Online Small Business Guide 2nd Ed.

DATA PRIVACY LAWS AND YOUR BUSINESS

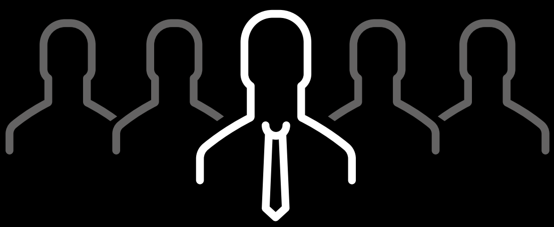
59%

of affected businesses are not aware of the new laws.

Despite new data breach notification laws coming into effect on 22 February, awareness around the new legislation in the business community is surprisingly low.

Only 1 in 5

small businesses aware of new legislation

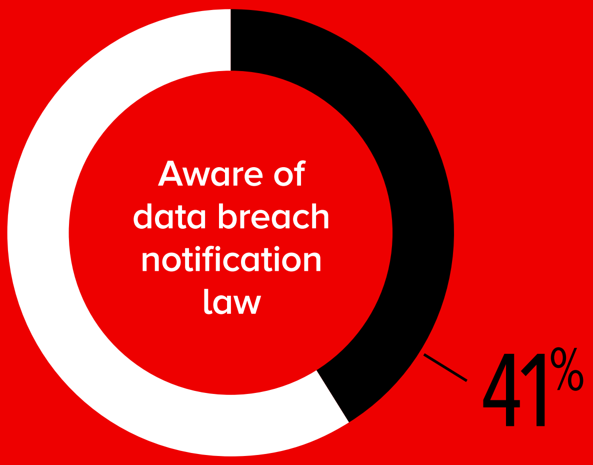


Smaller businesses that will be impacted by the changes to the Privacy Act are typically not familiar with the new laws or how it will impact their business.

There is a concerning lack of awareness with less than half of businesses (41%) affected aware of the incoming legislation. With small businesses being the least concerned about data security, they are also less likely to be aware and prepared for the new regulations with only 1 in 5 small businesses citing awareness. This is concerning given failure to comply puts private organisations with a turnover of more than $3 million at risk of crippling fines of up to $2.1 million.

BUSINESS SIZE BY EMPLOYEES	TOTAL	SMALL 1-19	MEDIUM 20-199	LARGE 200+
Prepared for data breach notification law (Average out of 10 pts)	**6.5**	5.1	7.0	7.3

Are you aware that a new mandatory data breach notification law is to take effect on 22nd February this year? – AFFECTED BUSINESSES ONLY (i.e., those that need to apply). On a scale from 0-10, how prepared do you think is your organisation to comply with the new law as outlined – AFFECTED BUSINESSES ONLY (i.e., those that need to apply). Base: Total (n=356), small (n=108), medium (n=103), large (n=145)



SMALL 1-19 EMPLOYEES	MEDIUM 20-199 EMPLOYEES	LARGE 200+ EMPLOYEES
19%	38%	59%

SAVE THE DATE
FEBRUARY 22, 2018

From 22 February 2018, amendments to the Privacy Act will make it obligatory for organisations covered by the Australian Privacy Act (this includes all Australian government agencies, and businesses and not-for-profit organisations with an annual turnover of $3 million or more), to notify certain breaches.

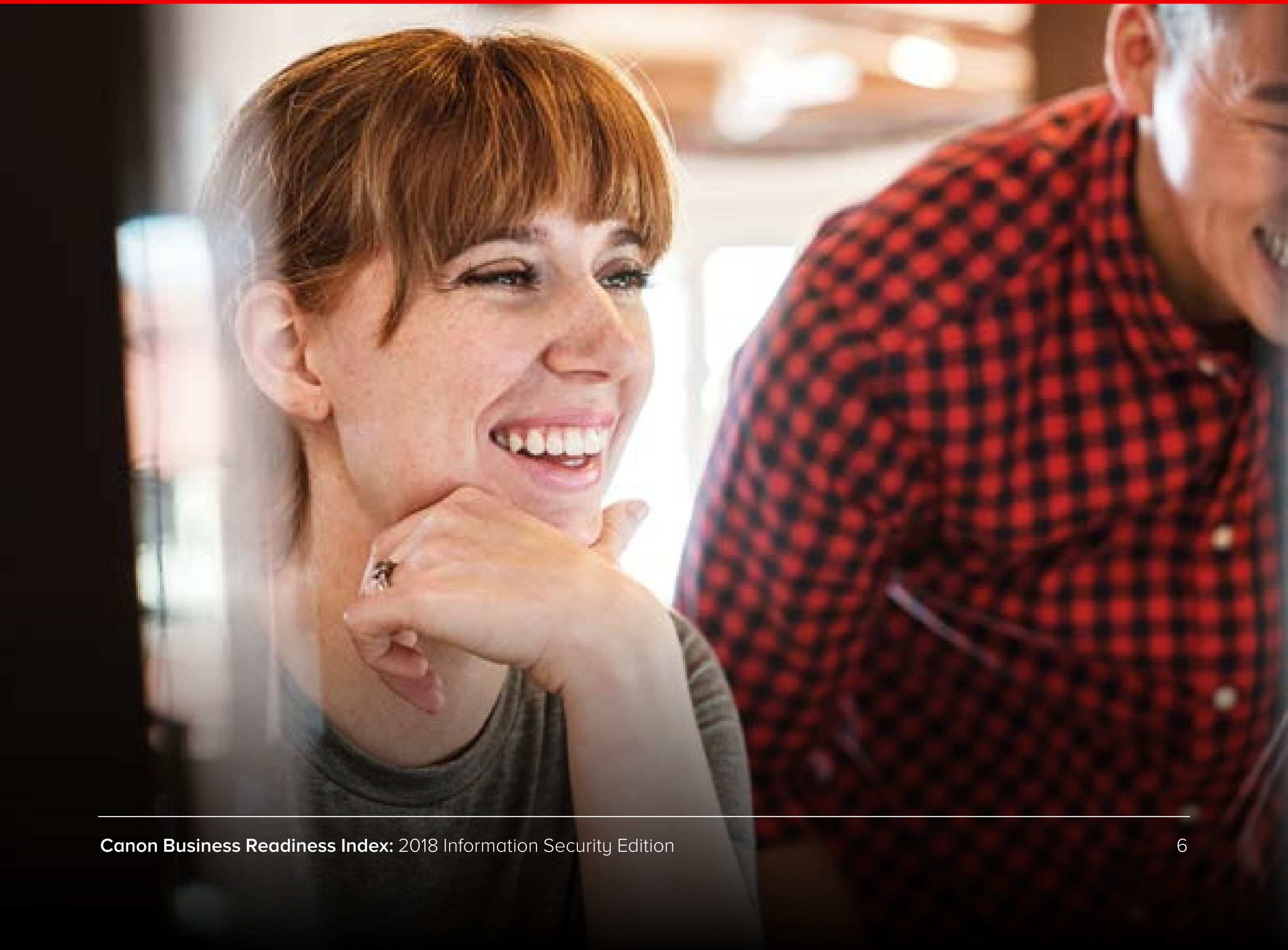
What is a personal information breach?

A personal information security breach refers to any unauthorised access or disclosure of the personal information your organisation holds. This also includes the loss of information that's likely to lead to unauthorised access or disclosure.

When do you need to notify?

The obligation to notify will apply if you have reasonable grounds to believe that:

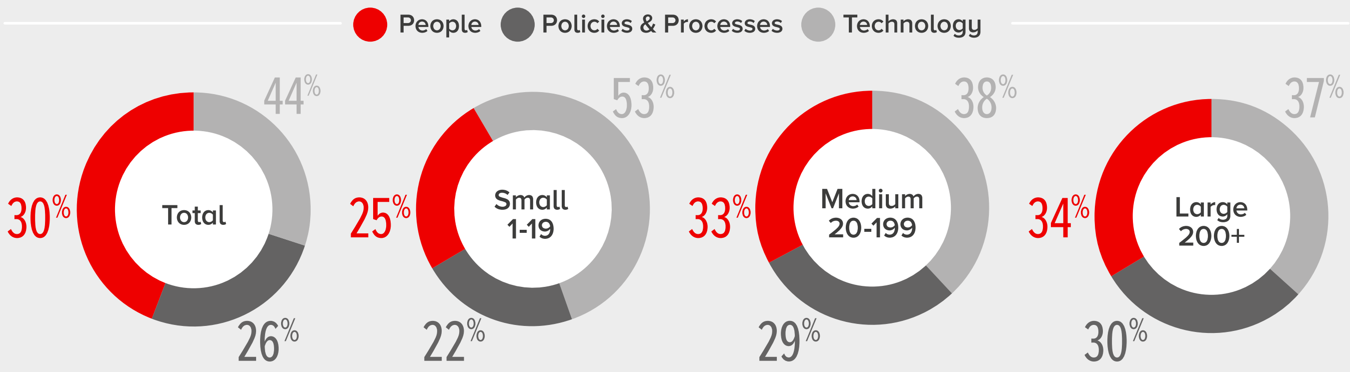
- a breach has occurred, and
- a reasonable person would conclude that the breach is likely to result in serious harm to the person that the information relates to.

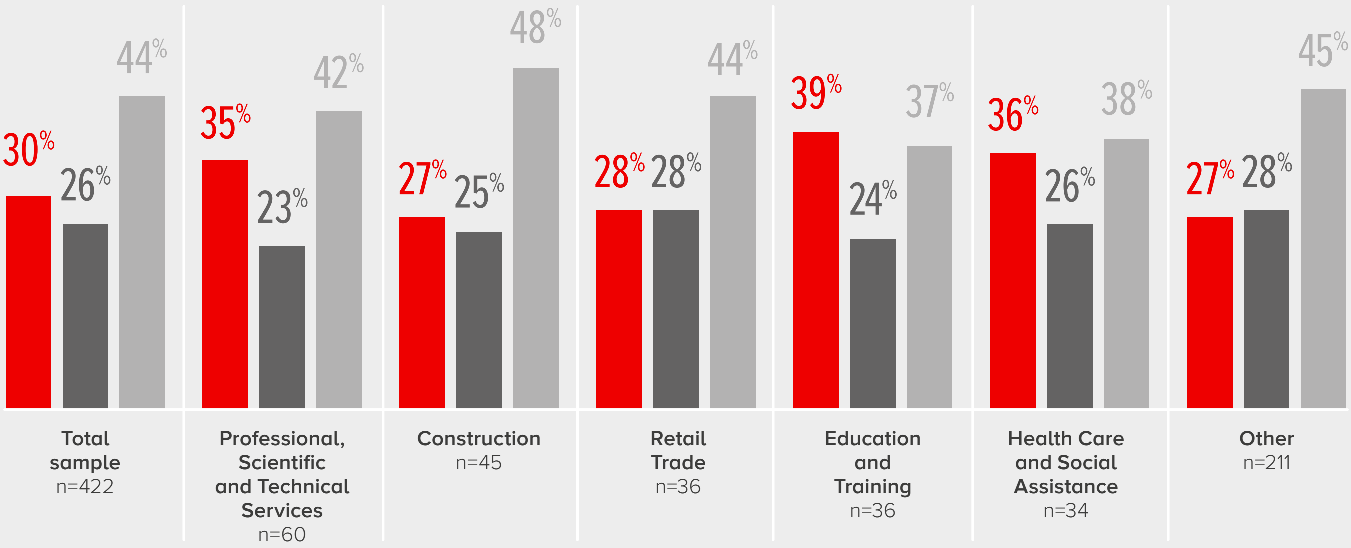


TECHNOLOGY SEEN AS **BIGGEST VULNERABILITY**

Across the board, businesses reported that technology was seen as the biggest vulnerability when it comes to assessing their security risks.

However, this trend changes as we look at larger businesses who have a more balanced view of their risks across people, processes and technology.





While medium and large businesses have a more balanced view of their security risks, small businesses are less aware of the risks to their business caused by their people and processes. The lack of awareness around the non-technological threats is a concern and creates a considerable vulnerability in the Australian business landscape – particularly for organisations that are partnering with small businesses that may not have comprehensive security measures in place. Employees in particular pose a huge threat to business' information security, whether that's by intentionally taking or unintentionally jeopardising information. Small businesses are just as vulnerable when it comes to the people in their business. 80% of hacking related data breaches involve weak or compromised passwords.[1] Making sure that your people understand the threats and are trained to help protect your business' information, will help you turn your weakest link into your best weapon against cyber-attacks.

Where do you think the biggest security risks lie within your organisation across the following three areas technology, processes, and people? People e.g. documentation, training compliance etc. Policies & Processes e.g. patch management, vulnerability scanning, privileges account management etc. Technology e.g. hardware & software to prevent data breaches e.g., access management system, intrusion detection etc. Base: Total (n=422), Small Business 1-19 empl (n=164), Medium Business 20-199 empl (n=108), Large Business 200+ empl (n=150), Professional, Scientific and Technical Services (n=60), Construction (n=45), Retail Trade (n=36), Education and Training (n=36), Health Care and Social Assistance (n=34), Other industries (n=211).

[1] Australian Government: Stay Smart Online Small Business Guide 2nd Ed.

THE RISKS BUSINESSES ARE MOST CONCERNED ABOUT

There is a seemingly ever-increasing range of security risks that are keeping IT managers and business owners awake at night. Around 1 in 2 businesses were found to be extremely/very concerned about the following risks.

Protecting company data

52%

Viruses

52%

Malware/spyware

51%

Protecting customer data

51%

Loss of personal identifiable information (PII) - customer or employee data

48%

External threat actors/groups (Hackers) stealing information/data

48%

Below are a number of security threats that other organisations have mentioned are a concern for them. For each, please indicate how much of a concern they are for your organisation. (% Extremely/Very Concerned). Base: Total (n=422), Small Business 1-19 empl (n=164), Medium Business 20-199 empl (n=108), Large Business 200+ empl (n=150).

MOST COMMON BREACHES

According to the study's participants, the most common security incidences that occurred in Australia in the last 12 months were:

1. Viruses
2. Spam
3. Malware/Spyware
4. Phishing
5. Ransomware

Those surveyed reported that on average it took **24.7 days** to detect a data breach.

> In fact, the global average is 94 days[2] to detect a security breach and in that time a cyber-criminal can get to know your business better than your IT department.

What type of security incidences have occurred at your organisation in the last 12 months? Base: n = 135 Thinking about the last data breach that occurred at your organisation, how long did it take to detect it? Base: n = 121.

[2] Asia Pacific Visa Security Summit 2015 20-21 May.

HOW IS YOUR **ESSENTIAL 8** LOOKING?

Many Australian businesses do not have adequate security measures in place.

Only 40%

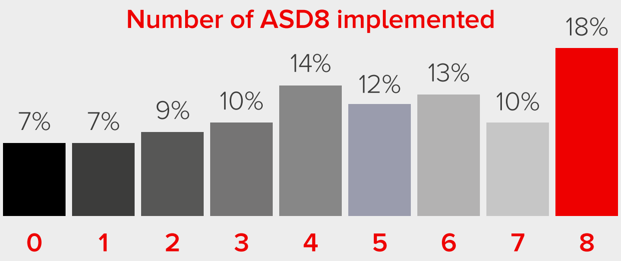
of Australian businesses have implemented six or more of the Australian Signals Directorate Essential 8 (ASD8) strategies to mitigate cyber security incidents and just 18% reported implementing all ASD8. Worryingly, 12% of small businesses in Australia have not implemented any of the ASD8.

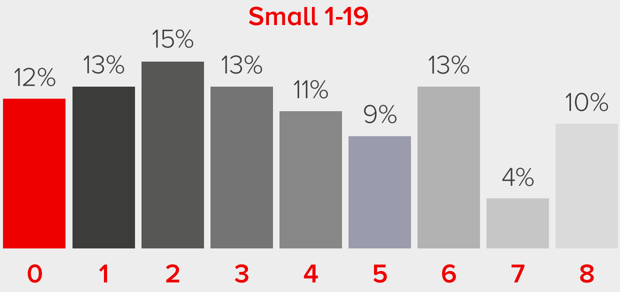
Small businesses are falling behind in terms of protecting their information security. This not only means their own information security is highly compromised, but they could be putting their suppliers' and customers' businesses at risk. This creates a significant hole in Australia's cyber security strategy as we are only as strong as our weakest link.

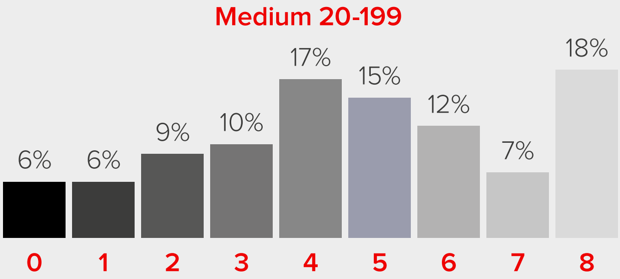
Australian businesses are not prepared enough when it come to their information security. The ASD8 outlines the key essential security measures that all businesses should have in place. Not having these strategies in place is like owning a bank and leaving the vault unlocked. The Australian Government offers some of the best cyber security resources in the world, they're free and all Australian businesses should be encouraged to make use of these. ASD8 is a good place to start.

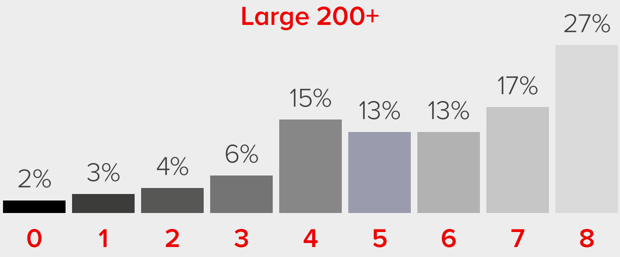
The Essential 8

- Application whitelisting
- Patch applications
- Disable untrusted Microsoft Office macros
- User application hardening
- Restrict administrative privileges
- Patch operating systems
- Multi-factor authentication
- Daily backup of important data


Number of ASD8 implemented


Small 1-19


Medium 20-199


Large 200+

Base: Total (n=422), Small Business 1-19 empl (n=164), Medium Business 20-199 empl (n=108), Large Business 200+ empl (n=150).

RISK MITIGATION STRATEGIES BY THE NUMBERS

Daily back up of important data is the most widely implemented cyber risk mitigation strategy, but print security is often being neglected.

Top 5 most common risk mitigation strategies:	% implemented
Daily backup of important data	70%
Threat and vulnerability scanning	65%
Someone directly responsible for security measures (e.g. response team/ capability)	62%
Business data loss prevention system	61%
Intrusion detection/ prevention systems	61%

Bottom 5 least common risk mitigation strategies:	% implemented
Mobile device management system	51%
Application Whitelisting (only selected software applications allowed to run on computers)	50%
Third party/ vendor risk assessments	50%
External certification to IT/ cyber security standards	49%
Print security controls (e.g. release to print via PIN or swipe card)	42%

Only 56%

of Australian businesses have been assessed for security risk management/IT security.

Businesses know they need to take action to protect themselves, but many don't know where to start. The first step in any business' security journey is to understand their unique situations and requirements, so they can put the right measures in place to suit their business. A security risk and management assessment should be the starting point for all businesses, yet only 56% have done so.

54%

of businesses that were recently assessed were highly concerned about security in their organisation.

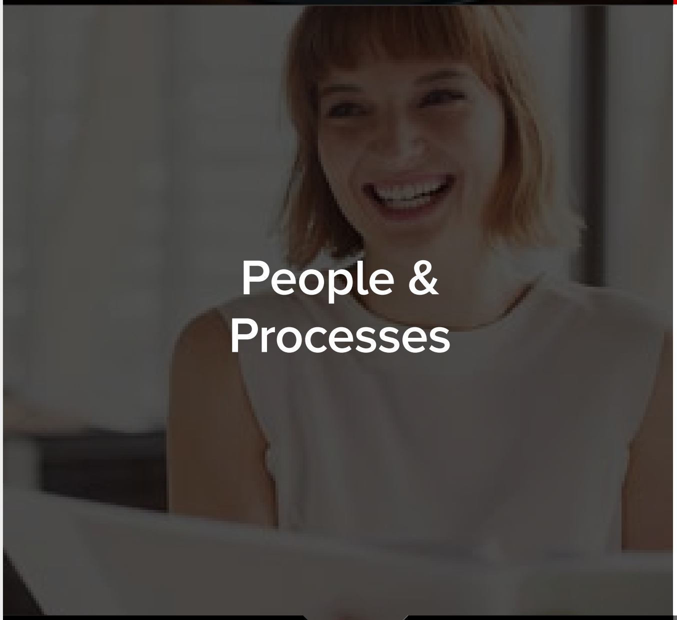
Compared to just 22% who hadn't been assessed. According to the research, larger businesses and those that had a security risk assessment were significantly more likely to have implemented ASD8s. 26% of businesses that reported being risk assessed had implemented all ASD8, compared to just 9% of businesses that had not been assessed.

Please indicate whether your organisation currently does or does not have in place any of the following %YES. Base: Total (n=422), Small Business 1-19 empl (n=164), Medium Business 20-199 empl (n=108), Large Business 200+ empl (n=150).

Print security

While 84%

of businesses are aware of printing-related security threats, only 4 in 10 businesses have their printers secured.



People & Processes

Small businesses (<20 employees) report the lowest rates of awareness around printer security issues – 31% are not aware of risks vs 5% of larger businesses (200+ employees).

Only 56%

of Australian businesses have a documented internal IT security/cyber security policy for employees, with only 55% investing in security training.

That rate drops for smaller businesses, with only 36% having policies in place and just 34% investing in security training.

Base: Total (n=422), Small Business 1-19 empl (n=164), Medium Business 20-199 empl (n=108), Large Business 200+ empl (n=150).

DATA SECURITY
SPENDING IS ON THE RISE

↑55%

of Australian businesses think their data security spend will increase in the next year by an average of 24%.

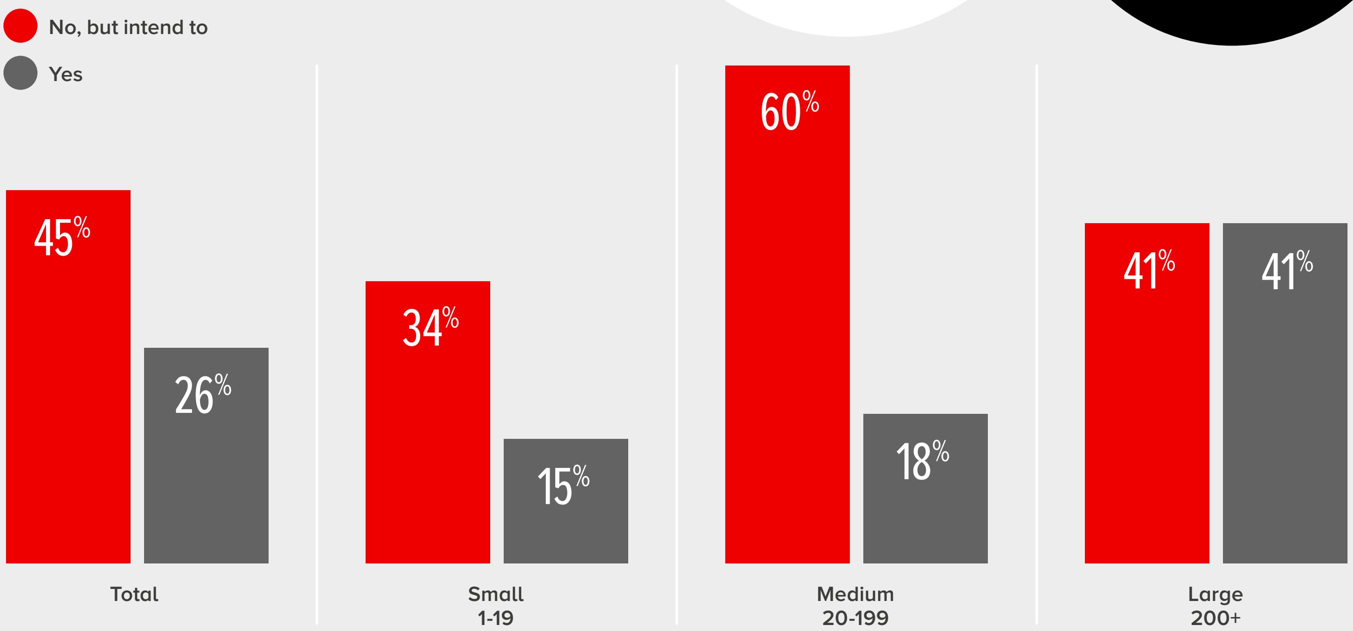
Owing to the new data breach notification laws coming into effect, 71% of businesses have, or intend to, put new systems in place to comply with the regulations. Smaller businesses are least likely to invest in new systems or processes.

> "Awareness, training, strengthen incident reporting, prevention and recovery".
>
> **CFO, B2C & B2B business, 100-199 employees**

> "The threats are becoming more complex. Turnover of staff is high which leads to important data being shared outside the company".
>
> **Operations Manager, B2C business, 250-300 employees**

> "[There is a] greater focus on cyber security by senior management".
>
> **IT director, B2C business, 500+ employees**

Due to the upcoming legislation has your organsiation put any new systems or processes in place to comply with the new regulations?



Base: Total (n=356), Small Business 1-19 empl (n=108), Medium Business 20-199 empl (n=103), Large Business 200+ empl (n=145).

NOTE ABOUT **THE STUDY**

The Canon Business Readiness Index: 2018 Information Security Edition is a comprehensive study that monitors and measures Australian business' digital readiness. The study, conducted by GfK Australia in January 2018, gathered insights from over 400 key decision makers from the Business and IT communities. The aim of the security study was to assess Australian businesses existing information security practices, and determine their preparedness and ability to comply with the new Data Breach Notification obligations coming into effect on 22 February 2018.

Managing your information security risks can be complex and challenging, but it doesn't have to be. Canon can work with you to help you understand your unique business requirements and develop a robust information security action plan that will keep your business safe.

To find out more contact:
Canon Australia Pty Ltd
Email: canongroup@canon.com.au
Phone: 1300 620 856
canon.com.au/business

No one does it like you

Canon