Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Security and Australian Small Businesses

Results from the Australian Cyber Security Centre Small Business Survey

cyber.gov.au

Table of Contents

Executive Summary

Australian businesses face increasingly sophisticated and capable cybercriminals targeting what matters most to them; their money, data and reputation. Bank accounts, email systems and business devices, including computers and mobiles, are just a few of the critical business assets that face compromise.

The Australian Signals Directorate's (ASD's) Australian Cyber Security Centre (ACSC) is acutely aware of the escalating scale and impact of malicious cyber activity. For the more than 2 million Australian small businesses[1] the actions of these malicious actors can be harmful, with some businesses unable to recover.

The ACSC acknowledges that Australian small to medium businesses (SMBs) operate in a different environment compared to larger enterprises, with 97% of Australian businesses having less than 20 staff. Managing competing business priorities with fewer resources, Australian small businesses require specific advice to better defend themselves from cyber security threats. While there are effective and inexpensive practices available to protect them against cyber incidents, many businesses are unaware these practices exist.

Recognising this gap, the ACSC partnered with the Behavioural Economics Team of the Australian Government (BETA) in 2019 to design the ACSC Small Businesses Survey (the Survey) and capture a baseline understanding of cyber security practices and knowledge of among Australian SMBs.

This report provides a summary and analysis of the data provided by respondents of the Survey with a particular focus on:

- The relationship between the size of an SMB and the decision to outsource their cyber security measures.
- The relationship between exposure to a cyber incident and the impact on subsequent evaluations of cyber-risk.
- The relationship between confidence in cyber security understanding and the cyber security practices of an SMB.

The report concludes that Australian SMBs know cyber security is important regardless of how they rate their understanding of cyber security. However, they face significant barriers when attempting to implement good cyber security practices. These barriers include a lack of dedicated staff with an IT security focus, the complex field of cyber security, challenges in understanding and implementing security measures, underestimating the risk and consequences of a cyber incident, and a gap in planning for, and responding to, cyber incidents.

Data from the Survey informed the development of the ACSC's technical guidance materials tailored to the needs and capabilities of Australian SMBs to help to protect them from cyber incidents. Specifically, data helped to tailor the security controls identified in technical guidance, the language used, and the way that content was structured to maximise retention and impact in an effort to protect Australian SMBs.

[1] Australian Bureau of Statistics, *8165.0 – Count of Australian Businesses, including entries and exits, June 2015 to June 2019*, 20 February 2020. https://www.abs.gov.au/AUSSTATS/abs@.nsf/Latestproducts/8165.0Main%20Features1June%202015%20to%20June%202019?opendocument&tabname=Summary&prodno=8165.0&issue=June%202015%20to%20June%202019&num=&view=

Executive Snapshot

Impact of cybercrime in Australia

1 report every 10 minutes

The ACSC receives approximately 144 reports of cybercrime a day.

$300 million per year

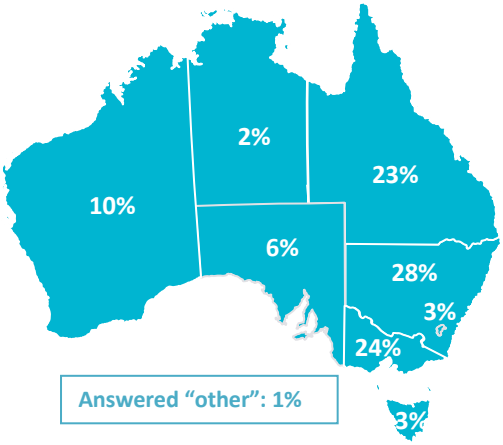
Estimated annual losses to cybercrime based on ReportCyber data.

Survey Responses

1763 responses

Across the nation the ACSC Small Business Cyber Security Survey received 1763 voluntary responses between June and September of 2019.

Respondents across Australia



What the ACSC considers an SMB

- Sole Trader – one employee
- Micro-business – two to four employees
- Small Business – five to 19 employees
- Medium-sized Business – 20 to 199 employees

Snapshot of the average respondent

Business owner

Responsible for their company IT

Cyber security incidents

- Has previously encountered a cyber security incident
- Considers it ‘likely’ or 'almost certain' to happen in the future
- Thinks they could regain normal operations within a few days if it

Devices

- Use a Windows desktop computer
- Use an Apple iPhone

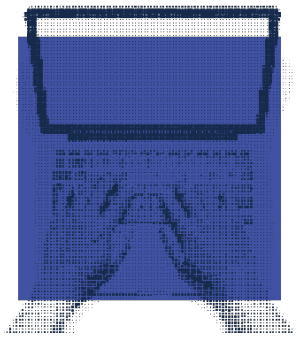
Rates cyber security

- As ‘important’ to ‘very important’ to their business
- ‘Average’ or ‘below average’ understanding of cyber security

Software

- Use Microsoft Office for day-to-day operations

Key findings



62% have been victims

62 per cent of respondents have experienced a cyber security incident.

Cyber security is important

80 per cent rated cyber security as ‘important to very important’.

1 in 5 unaware of phishing

1 in 5 SMBs did not know the term “phishing”.

Vulnerable cohort

SMBs that outsourced IT security believe they are better protected than they really are.

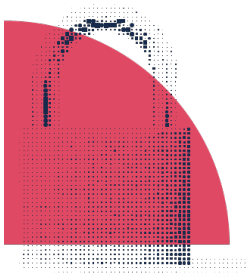
Low level of understanding

Almost half of SMBs rated their cyber security understanding as ‘average’ or ‘below average' and had poor cyber security practices.

$500 spent on cyber security

Almost half of SMBs reported they spent less than $500 on cyber security per year.

Barriers to implementing good cyber security practices



Lack of dedicated IT staff

Cyber security has to compete for time and other resources with multiple demands.

Planning & responding

Businesses need to better plan for and respond to cyber incidents.

Complexity & self-efficacy

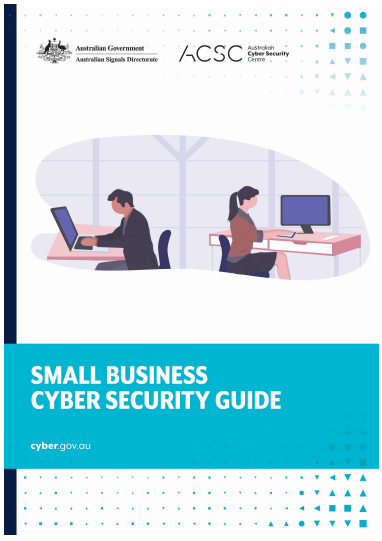
Business owners fail to identify weaknesses in security practices and know they are struggling, but do not know where to begin.

Underestimate risk

Businesses need to better understand the risk and impact of a cyber incident and to not underestimate their recovery period from a cyber incident.

Guidance produced based on data from the ACSC Small Business Survey

Data from The Survey informed the development of technical guidance materials tailored to need of small businesses.



Methodology

The Survey was published on the ACSC's cyber.gov.au website, available to businesses and promoted online with the assistance of national peak bodies and industry associations, as well as the Australian Taxation Office and the Department of Industry, Science, Energy and Resources.

The ACSC adopted the Australian Bureau of Statistics' definition of business size to define an SMB, which relates to the number of employees:

- Sole Trader — one employee
- Micro-business — two to four employees
- Small Business — five to 19 employees
- Medium-sized Business — 20 to 199 employees.

Participation was optional with no incentive provided to complete the Survey. Data was provided through an online survey platform via 55 multiple choice questions that took roughly 12 minutes to complete.

Questions were designed to gather an understanding of cyber security practices and knowledge among Australian SMBs, testing a range of topics from types of devices used by businesses to understanding of key cyber security terms.

The Survey collected responses from June 2019 to September 2019 and collected 1763 responses.

Results

Key findings

Survey respondents

Survey respondents closely reflect the proportions of businesses across states and territories (Figure 1) and provides a robust snapshot of industry sectors across Australia (Figure 2). Not surprisingly, data shows that the largest number of survey respondents are from industry sectors that rely heavily on digital capabilities for their operations. This suggests that these industries are more likely to stay informed of initiatives and information on cyber security, such as the Survey, than industries who do not rely so heavily on digital capabilities for their operations. These sectors include Professional, Scientific and Technical Services, Retail Trade, Information Media and Telecommunications and Construction.

Micro businesses (two to four employees) comprise the largest group of respondents with respect to business size, while sole traders were less likely to participate in the Survey compared to larger businesses (Figure 3).

Figure 1: Distribution of businesses by State and Territory

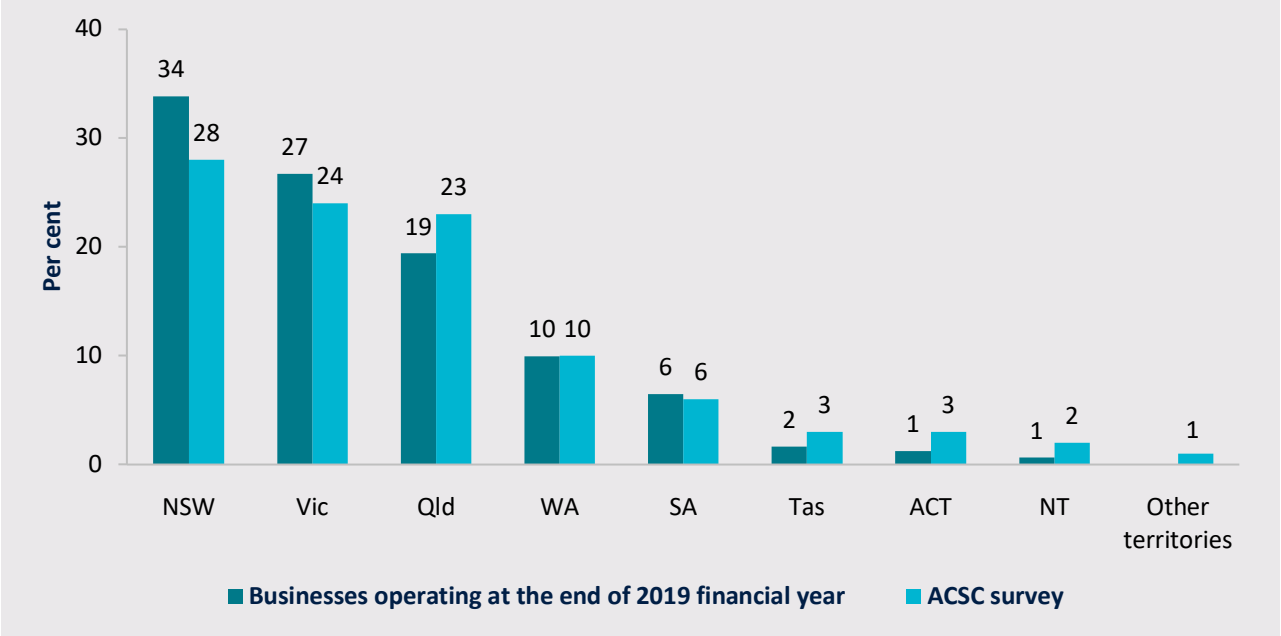
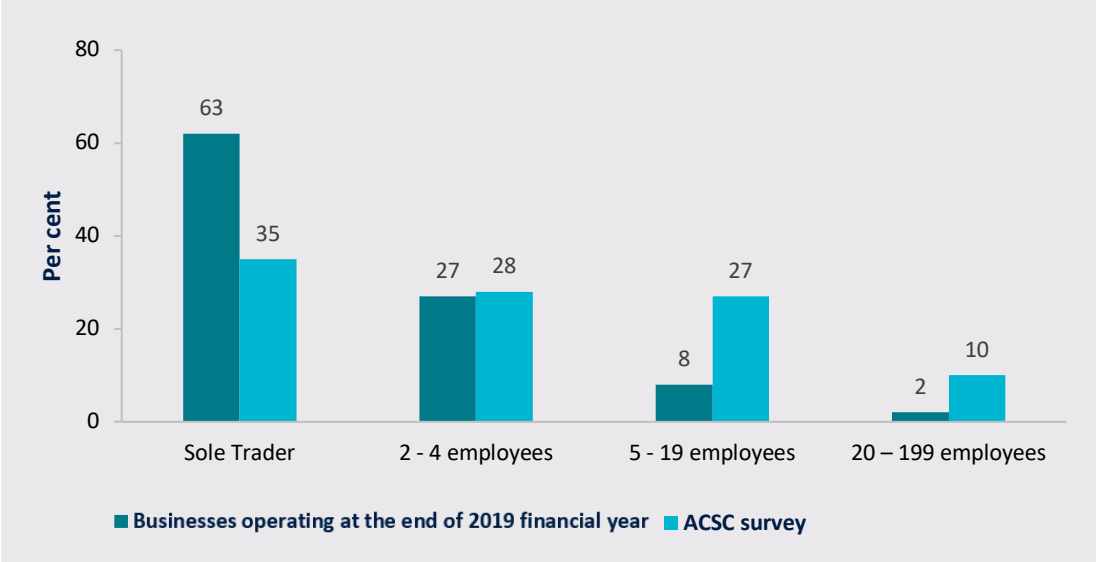


Figure 2: Sample distribution by industry

Industry	Number of participants	Per cent
Agriculture, Forestry and Fishing	88	5
Mining	20	1
Manufacturing	89	5
Electricity, Gas, Water and Waste Services	22	1
Construction	147	8
Wholesale Trade	53	3
Retail Trade	174	10
Accommodation and Food Services	57	3
Transport, Postal and Warehousing	30	2
Information Media and Telecommunications	151	9
Financial and Insurance Services	118	7
Rental, Hiring and Real Estate Services	37	2
Professional, Scientific and Technical Services	301	17
Administrative and Support Services	52	3
Public Administration and Safety	12	1
Education and Training	53	3
Health Care and Social Assistance	104	6
Arts and Recreation Services	42	2
Other Services	213	12
Total	**1763**[2]	**100**

[2] Three respondents left this field blank but continued to answer other questions.

Figure 3: Sample distribution by business size (based on number of employees)



Self-assessment of cyber security

The average respondent was the business owner, responsible for the business' IT, and rates cyber security as very important to their business but considers their understanding of cyber security to be average or below (Figure 4). The majority (97 per cent) of respondents view cyber security as important to their business, higher than the proportion that view physical security as important (92 per cent). This view remains consistent, regardless of whether respondents perceive themselves to have an 'average' or 'above average' understanding of cyber security. This shows that Australian SMBs recognise that cyber security is important, regardless of their level of understanding.

SMBs that had previously experienced a cyber incident are much more likely to assess the future likelihood of a cyber incident as probable. 72 per cent believe it 'likely' or 'almost certain', compared to 25 per cent of SMBs that had never experienced a cyber incident).

In the event of a cyber incident, 87 per cent of SMBs believe they could regain normal operations immediately or within a few days.

Australian SMBs know cyber security is important, regardless of how they rate their level of understanding

Figure 4: Characteristics of respondents

Average respondent profile

- Business owner – 77%
- Responsible for company IT – 75%
- Uses an Apple iPhone – 59%
- Uses a Windows desktop computer – 66%

Average respondent rates

- Cyber security as 'very important' to their business – 80%
- Their cyber security understanding as average – 40%

Average respondent's cyber security incidents

- Previously encountered a cyber security incident – 62%
- Consider it 'likely' or 'almost certain' to happen in the future – 54%
- Thought they could regain normal operations within a few days if it does – 46%

Cyber security spending

SMBs spend little on cyber security, with nearly half (48%) of businesses reporting they spend less than $500 on cyber security per year. Nearly a fifth of SMBs spend between $500–$999 per year and another fifth spend $1000–$4,999 annually, while six per cent of SMBs are unsure what they spent on cyber security (Figure 5).

Low spending is perhaps explained by the fact that half of all SMBs that responded earn less than $250,000 annually (Figure 6). It is likely that the amount SMBs spend on cyber security is influenced by annual turnover, with those that earn more are able to spend more on cyber security. While increased spending does not necessarily correlate to increased security, it demonstrates higher prioritisation of cyber security in business operations.

Figure 5: Annual cyber security expenditure (per cent)

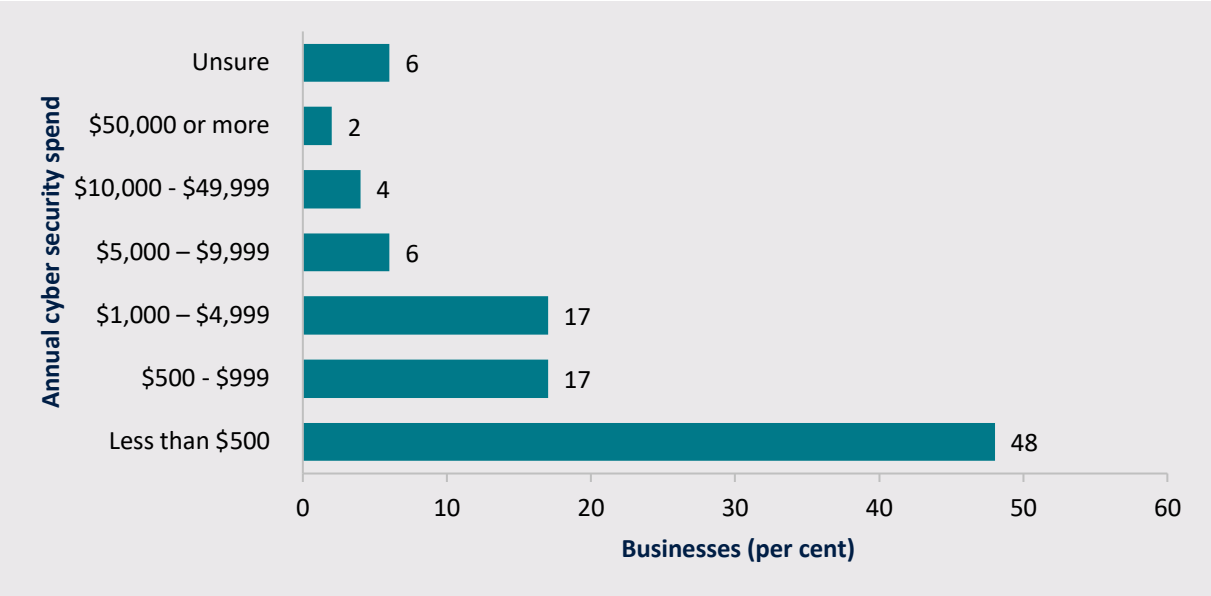
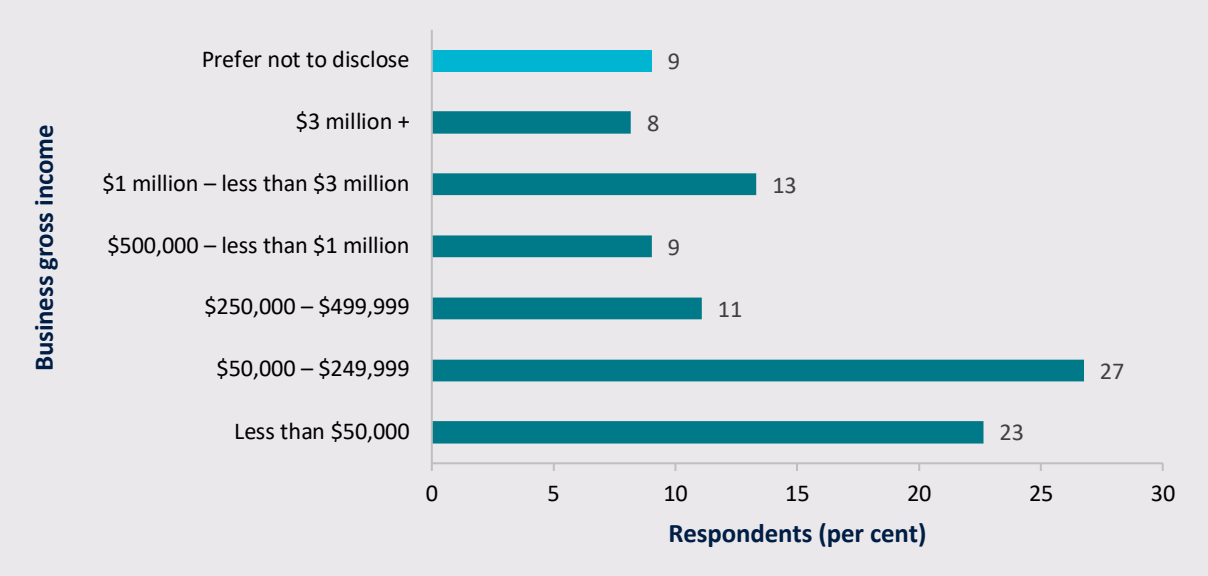


Figure 6: Percentage of responding SMBs by gross income category



Use of devices

Email is the most commonly used method for SMBs to communicate with their customers, while Apple iPhones are the most popular smart device used to conduct day-to-day business operations. Authentication tokens for two-factor authentication, and EFTPOS machines are also popular among SMBs.

Sole traders and micro businesses are more likely to use portable devices such as laptops, however, as businesses became larger, they are more likely to transition to desktops.

Almost 90 per cent of SMBs use Microsoft Office for their day-to-day operations with slightly less using some form of anti-virus software. Data shows that 22 per cent of SMBs use a password manager, and those who rated themselves with an 'above average' understanding of cybersecurity are twice as likely to use a password manager than those who rated themselves with 'average' or 'below average' understanding of cyber security.

Windows 10 followed by Windows 7 (which became unsupported from January 2020) are the most widely used operating systems by SMBs owning a PC, while Mojave followed by High Sierra are the most popular operating systems used SMBs owning a Mac. Of the SMBs using a Mac, around one in five are unaware what operating system they use. For SMBs using a PC, one in four use an operating system version that is Windows 7 or older.

Overall, Australian SMBs fall short in understanding what operating systems they use and how to keep their operating systems up to date. These findings led the ACSC to tailor guidance to advise SMBs how they can check what operating system they use and configure automatic backups on their devices..

Nearly one in five SMBs that use a Mac are unaware what operating system they use

One in four SMBs that use a PC use an operating system version that is Windows 7 or older

Areas of Interest

Spread too thin? Outsource to specialists, or adopt the DIY approach

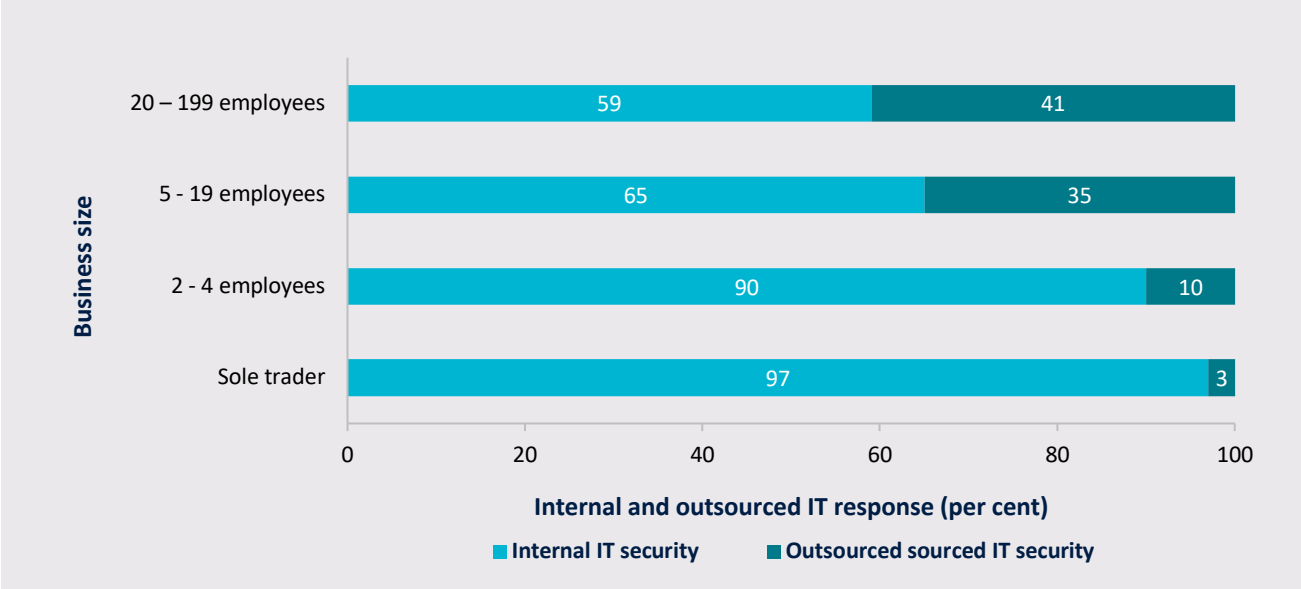
The Survey shows nearly half of SMBs spend less than $500 dollars annually on cyber security. This suggests that many SMBs take a DIY approach. However, cyber security is a complex field with rapidly evolving technology and increasingly sophisticated cybercriminals pushing boundaries. The Survey sought to understand whether SMBs that adopt the DIY approach generally implement the basic steps that will minimise their risk of a cyber incident. Further, the Survey sought to understand how much outsourcing buys peace of mind for SMBs, when in fact they may not be as protected as they believe.

Outsourcing is not a popular option for SMBs. In fact, 97 per cent of sole traders take matters into their own hands, while in contrast, 41 per cent of medium sized businesses choose to outsource as a support service (Figure 7). This suggests a relationship between business size and the decision to outsource. The larger the business, the more likely they are to outsource as a support service.

Another factor that impacts the decision to outsource as a support service is annual turnover. Data shows that once annual turnover reaches $250,000 dollars or higher, businesses begin to outsource, demonstrating the decision is influenced by financial capacity as well as security needs. Another variable that may impact the decision is workload management, with some SMBs drawn to outsourcing simply because it lightens their workload and means another party is responsible for the task.

97 per cent of sole traders adopt a DIY approach

Figure 7: Responsibility for IT security management by business size (per cent)



SMBs that chooses to outsource may not be as protected as they believe

SMBs that outsource may not be as protected as they believe. Outsourcing may lead to gaps in the owner's cyber security knowledge about which security measures are being implemented to protect their business. Data shows that for many SMBs opting to outsource, their outsourced provider did not necessarily implement all of the Essential Eight Mitigation Strategies [3](Figure 8) – the ACSC's prioritised list of mitigation strategies to assist businesses in protecting their systems against a range of adversaries. However, SMBs that outsource are more likely to conduct daily backups of their information.

Of SMBs that adopt a DIY approach, most implement one to five of the Essential Eight Mitigation Strategies. Results showed that when measured against the Essential Eight Mitigation Strategies, medium sized businesses were more likely to implement a majority of strategies (44 per cent) compared to businesses with fewer than 20 employees (30 per cent).

Medium sized businesses implemented more of the Essential Eight Mitigation Strategies than small businesses

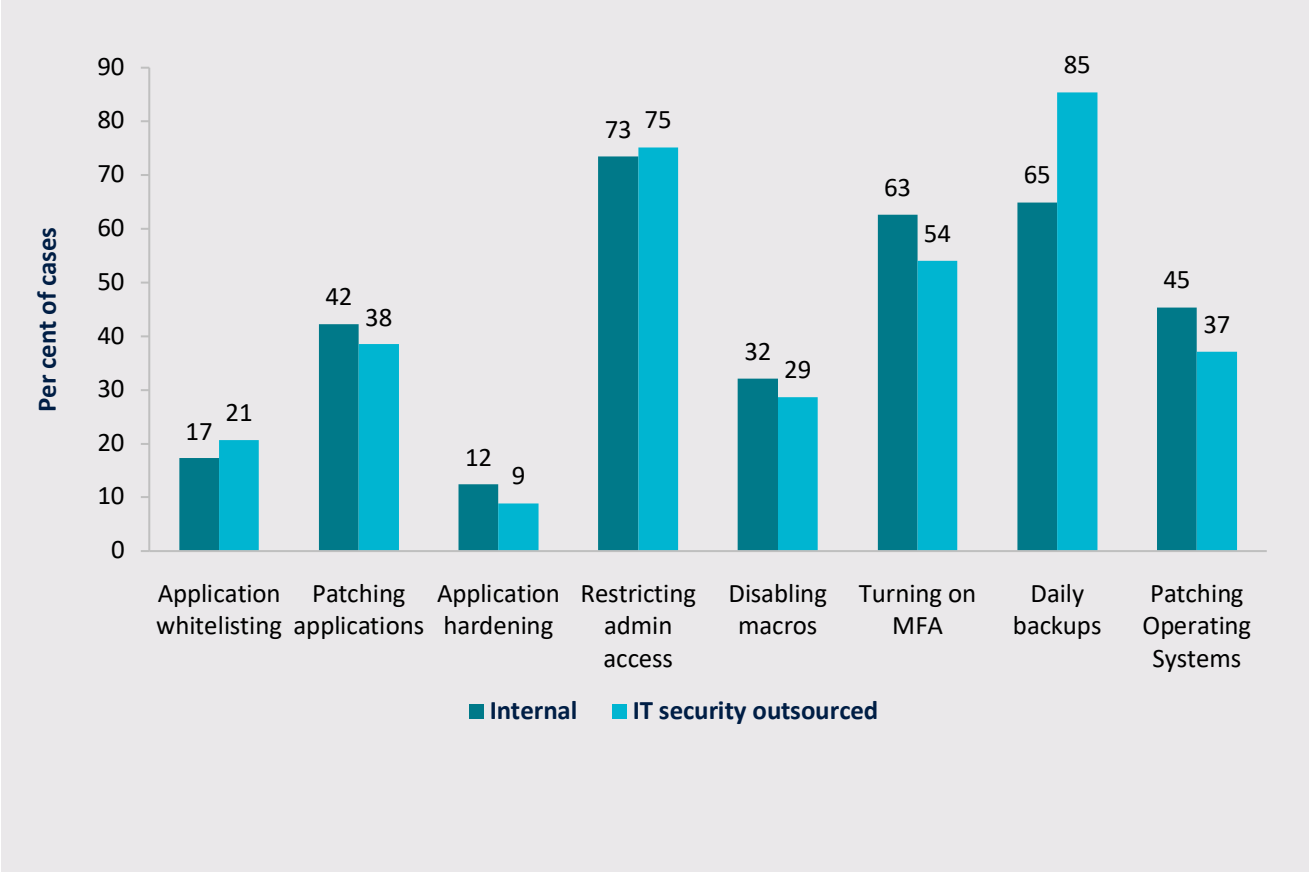
While the Essential Eight Mitigation Strategies are not guaranteed to prevent 100 per cent of cyber incidents, they provide a useful benchmark to measure the cyber security posture of Australian industry. In addition to making it harder for adversaries to compromise systems, implementing the Essential Eight Mitigation Strategies can be more cost-effective for SMBs in terms of time, money and effort than having to respond to a cyber security incident. This difference is evident in responses to the survey question about automation of backups, in which backups are automated in 72 per cent of SMBs that choose to outsource compared to 52 per cent that adopt a DIY approach. By making it clear to SMBs that backups can be automated, and demonstrating how many business owners or staff can do this with little cost or technical training, an SMB's ability to more quickly recover after ransomware cyber incidents can be substantially improved.

SMBs with greater confidence in their cyber security understanding are more likely to adopt a DIY approach. If an SMB rates themselves to have an 'expert' understanding of cyber security, they are less like to outsource (seven per cent). Sixty per cent of SMBs rate their understanding as 'average' or 'below average', of which 20 per cent are more likely to choose to outsource. This indicates that those SMBs that currently outsource could have worse cyber security if they tried to manage it themselves.

Overall, data shows that SMBs might believe they are better protected than they actually are if they choose to outsource. This insight is supported by the fact that a large proportion of businesses who outsource have low implementation of the Essential Eight Mitigation Strategies.

[3] https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-maturity-model-faq

Figure 8: Essential Eight Mitigation Strategies applied by whether businesses outsource their IT security



Evaluating cyber risk on an ongoing basis

For SMBs, a cyber incident can be harmful, with some SMBs unable to recover. The Survey sought to understand how SMBs might accurately evaluate their risk of a cyber incident.

Some cyber risks are more common than others; for example, many SMBs regularly receive scam emails or text messages. While attempts might occur frequently, business owners might not know there was a near-miss if they are often prevented by security measures from reaching end users. Further, because long periods, often years, can pass without a cyber incident, it can be difficult for SMBs to accurately assess their risk of a cyber incident.

People are generally better at evaluating the likelihood of things that happen often, compared to things that happen rarely (this is sometimes referred to as the availability heuristic or availability bias). Coupled with the unique context of each SMB operating via different digital methods and a rapidly evolving cyber threat landscape, evaluating the risk of a cyber incident is a challenging task for any business.

BOX 1: COMMON BIASES INFLUENCING CYBER SECURITY PRACTICE

The availability heuristic (also called the availability bias) is a mental shortcut for processing information or making decisions based on things that easily come to mind. Instead of making a decision based on the true likelihood of an event, the availability heuristic can lead people to overestimate the likelihood of something happening because we can recall examples a similar event.

Among SMBs surveyed, experiencing a cyber incident impacts the level of concern about and actions against cyber incidents in the future.

Unfortunately, experiencing a cyber incident is common for Australian SMBs. Of those surveyed, 62 per cent had experienced a cyber incident. Incidents are more common among businesses with five or more employees, affecting around three quarters of small (5-19 employees) and medium (20-199 employees) businesses. For sole traders and micro businesses, over half of those surveyed had experienced a cyber incident.

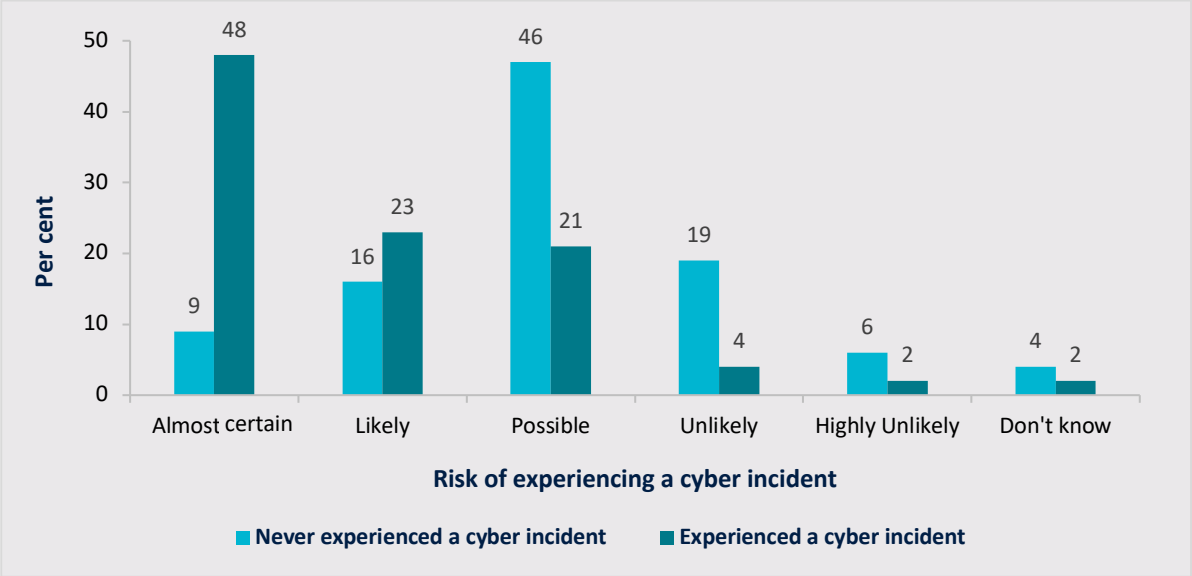
Experiencing a cyber incident changes an SMB's evaluation of risk. Those that experienced a cyber incident consider the likelihood of a future incident 'almost certain', while those who had never experienced a cyber incident consider the likelihood 'possible' (Figure 9). SMBs that experienced a cyber incident are also more likely to rate cyber security as 'very important' (83 per cent compared to 75 per cent of SMBs who had never experienced a cyber incident). This suggests that once an SMB has experienced a cyber incident, they become more aware of the risk, view cyber security as more important, and believe that a cyber incident would occur again.

Most SMBs (almost 9 out of 10) estimate that they will recover from a cyber incident 'immediately' or 'within a few days', regardless of whether they had previously experienced a cyber incident. Reports to the ACSC (an average rate of one report every 10 minutes) show that businesses commonly underestimate their cyber incident recovery period. Further, not all cyber incident recoveries are whole. Many businesses only partially recover, permanently losing critical data or finances.

In addition, SMBs who have experienced a cyber security incident are more likely to choose to outsource (20 per cent) compared to businesses who had not (11 per cent). This suggests that experiencing a cyber incident motivates a business to take further action, such as outsourcing to a security provider.

Australian SMBs underestimate their recovery time from a cyber incident

Figure 9: Self-assessed risk of experiencing a cyber incident in the next 12 months



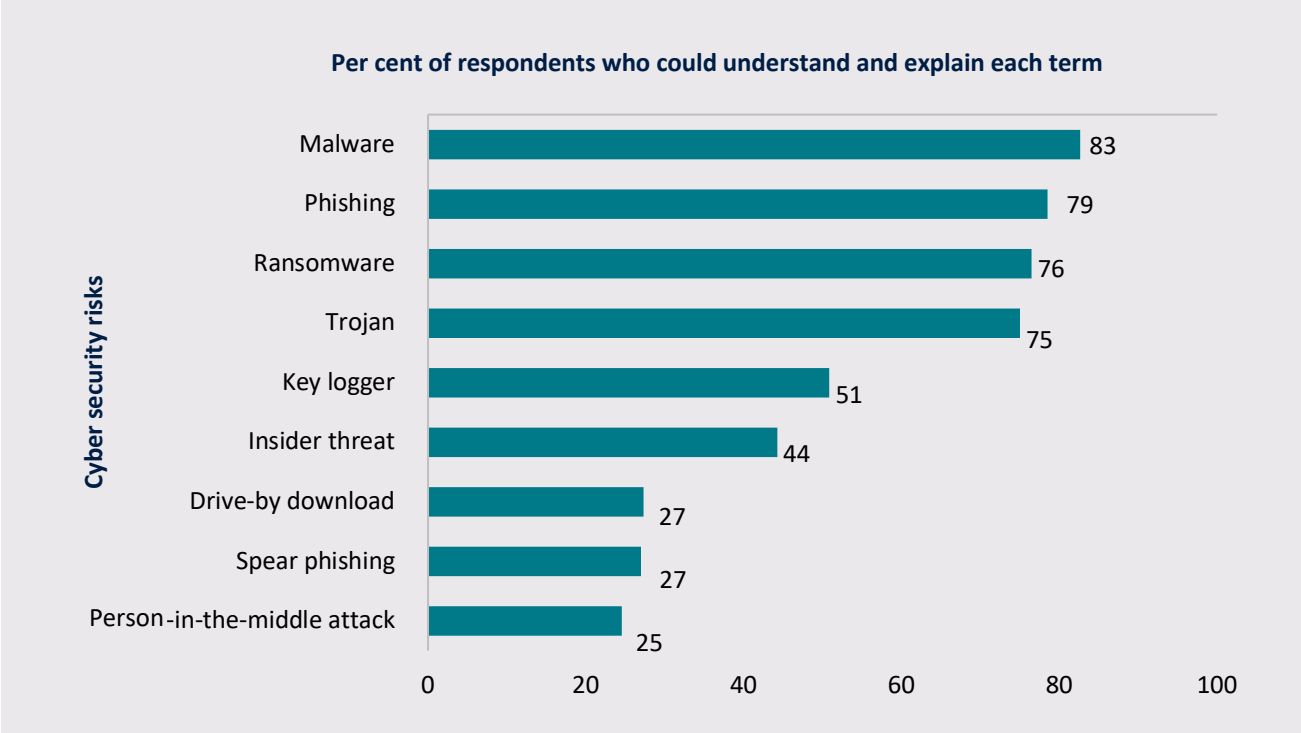
Can SMBs accurately evaluate their cyber-expertise? The relationship between confidence and cyber security

A significant portion of the survey focussed on gathering data about which cyber security risks Australian SMBs understand and feel confident explaining to staff and customers. Understanding cyber security risks is a critical step in recognising, responding to, and recovering from a cyber incident. It helps SMBs mitigate the impact of a cyber incident and determine which security practices to implement.

Data shows that Malware, Phishing and Ransomware are the most commonly understood cyber security risks (Figure 10). Nearly one in ten respondents feel they are unable to explain any of the cyber risks listed: these being Malware, Phishing, Ransomware, Trojan, Key logger, Insider Threat, Drive by download, Spear phishing, and Person-in-the-middle attack (Figure 10). Conversely, only 15 per cent feel they can explain all nine cyber risks identified by the survey (Figure 12). Overall, knowledge of cyber security risks among Australian SMBs is low.

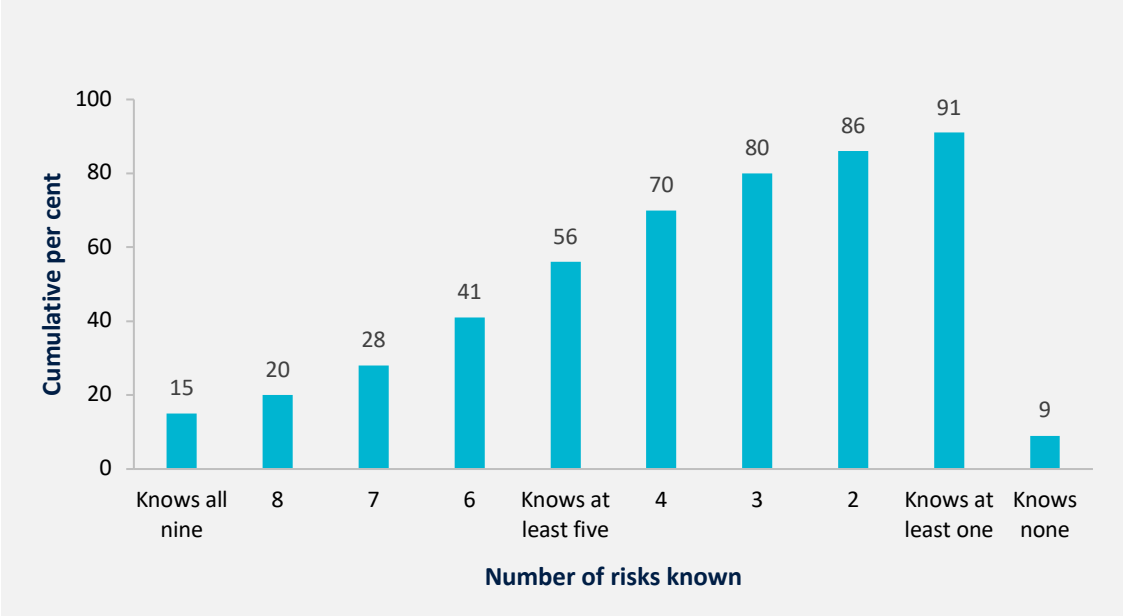
Nearly one in ten respondents felt unable to explain any of the cyber risks listed

Figure 10: Can SMBs understand and explain cyber security risks?



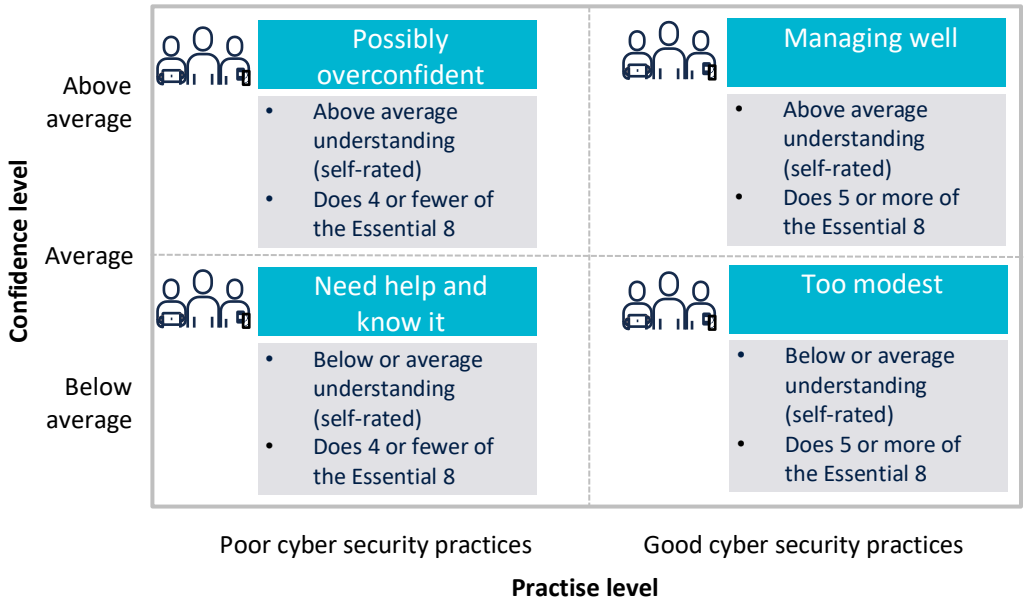
1 in 5 SMBs did not know the term "phishing", a type of dodgy email designed to trick recipients out of money and data

Figure 11: How many of the nine cyber risks are businesses able to understand and explain?



To better understand the relationship between confidence and cyber security practices, the Survey measured how SMBs rate their cyber security understanding (below average to above average) against how many of the Essential Eight Mitigation Strategies businesses they implement. The Survey examined whether SMBs rate themselves as a cyber expert (above average knowledge) against whether they implement five or more of the Essential Eight Mitigation Strategies and grouped respondents into 'confidence profiles' (Figure 12).

Figure 12: Cyber security confidence profiles



Almost half of SMBs rate their cyber security understanding as 'average or below' and had poor cyber security practices (implement four or fewer of the Essential Eight). They were categorised as 'needing help and know it'. Almost a quarter of SMBs are 'managing well' (implemented five or more of the Essential Eight). Nine per cent of SMBs are 'too modest' in their assessment of cyber security understanding but have 'good cyber security practices', while one in five SMBs are 'possibly overconfident' (implement 4 or fewer of the Essential Eight) (Figure 13).

Figure 13: Percentage of SMBs falling within each confidence profile

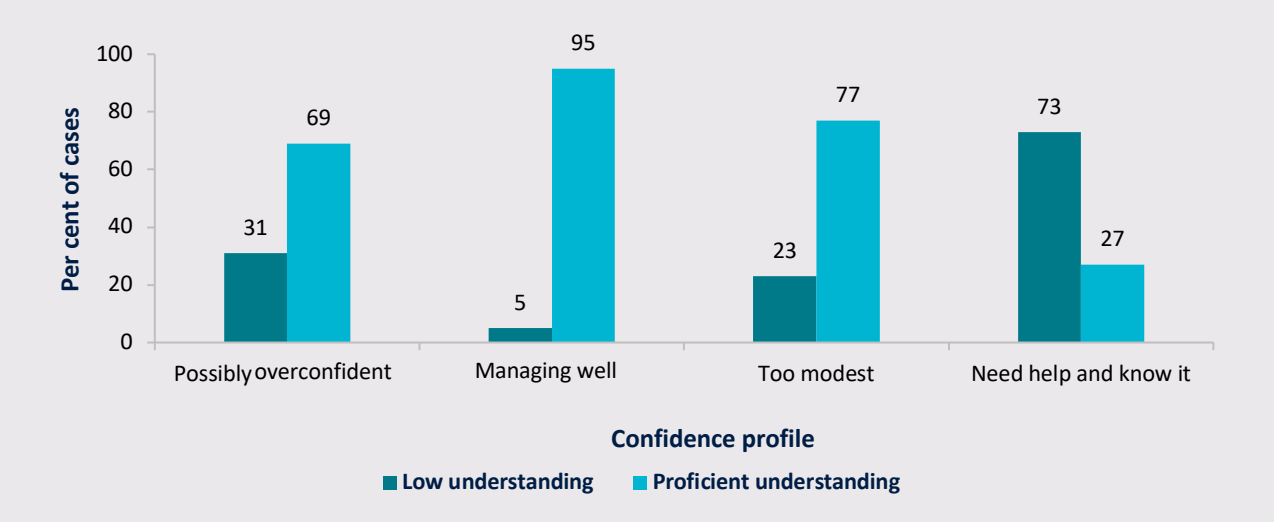
Only 69 per cent of SMBs that are 'possibly overconfident' have a proficient understanding of cyber security risks (Figure 15). This can be compared to 95 per cent of SMBs with 'managing well' and a proficient understanding of cyber security risks. Only one in four SMBs who 'need help and know it' have a proficient understanding of cyber security risks. Overall, more SMBS with 'high confidence and good practice' can explain cyber security risks than businesses who are 'overconfident with poor cyber security practices'.

While confidence in cyber security understanding implies willingness to take action, the problem with 'overconfidence' in cyber security understanding is that it is more likely to lead to errors or complacency as SMBs believe they are either not at risk of a cyber incident or they have appropriate measures in place to protect their business. Over confidence in cyber security understanding generally increases risk of a cyber incident. Similarly, low confidence in cyber security understanding can be negative, as SMBs feel they are ill-equipped to understand cyber risks or take action to implement cyber security practices to protect their business. Accurate self-assessment of cyber security understanding and a willingness to adopt new cyber security practices are critical components to help protect Australian SMBs against cyber incidents.

BOX 2: COMMON BIASES INFLUENCING CYBER SECURITY PRACTICE

Optimism bias and overconfidence refers to our tendency to be unrealistically optimistic even when the stakes are high. This may lead people to downplay risks and overestimate their own ability.

Figure 14: The relationship between confidence and understanding of cyber security risks



BOX 3: COMMON BIASES INFLUENCING CYBER SECURITY PRACTICE

Decision making can be thought of as following two modes: automatic, fast, and non-conscious (or "System 1" thinking), or controlled, slow, and conscious (or "System 2" thinking). Although our "fast" system is efficient for everyday decisions, our mental shortcuts can sometimes lead to cognitive biases. Email checking behaviour, when we may click links or open attachments without pausing to think can make us susceptible to scams.

Operating Systems

Promisingly, less than one in four SMBs that own a PC use an operating system older than Windows 8. However, for Apple users, almost a quarter of SMBs (22 per cent) did not know what operating system version they were using at all.

Not knowing which type of operating system you are using, or using older versions of operating systems, increases the risk of cyber incidents for SMBs. When software is no longer supported by security updates by the manufacturer malicious actors have more time to exploit security flaws that will never be fixed. Updates (or 'Patches') are new, improved or fixed versions of software installed on your computers or mobile devices. In the case of Windows, Windows 7 was no longer supported from January 2020. While some SMBs in the survey may have planned operating system upgrades prior to this deadline, it is likely many were unaware of their operating system End of Support date.

Overall, data shows that Australian SMBs need a greater understanding of which versions of operating systems they were using and their End of Support arrangements.

ICT products have life cycles through which they are supported by updates from their manufacturer to maintain security.

Conclusion

Australian SMBs know cyber security is important, but there are barriers to implementing good practices

The Survey revealed that Australian SMBs across states and territories, industry sectors, and business sizes have varying levels of cyber security understanding which impacts the quality of cyber security practices they implement.

Overall, Australian SMBs know cyber security is important regardless of how they rate their level of cyber security understanding, but they face barriers when attempting to implement good cyber security practices. These include:

- **Not having dedicated staff with an IT security focus**. Cyber security has to compete for time and other resources with multiple demands. The ability to outsource to experts is also impacted by financial capacity as well as security needs. If SMBs do outsource, they may not be as protected as they believe.
- **Complexity and self-efficacy**. SMB owners may think they are doing enough, but fail to identify weaknesses in their security practices. They may also know they are struggling, but do not know where to begin or what to do about it. Cyber risks and cyber security best practices change over time, so learning must be ongoing with cyber risks and behaviours continually monitored. Further, language used in available cyber security guidance may be too technical, so security controls may be difficult to grasp let alone implement. This demonstrates the importance of cyber security guidance that contains easy-to-understand, principles-based language that SMBs can action effectively.
- **Underestimating the risk and consequences of a cyber incident**. Australian SMBs need to better understand the risk and impact of a cyber incident. They underestimate their recovery period from a cyber incident, and those who have never experienced a cyber incident consider one less likely to occur. SMBs also face the inherent problem of a lack of positive reinforcement for good cyber security practices and cannot learn from near misses if their security practices are effective in preventing an incident from occurring. The ad hoc and intermittent nature of cyber incidents also complicates an SMB's ability to accurately evaluate cyber risks and results in the availability bias.
- **Planning and responding**. SMBs need to better plan for and respond to cyber incidents. While some cyber security measures can be planned in advance, like automating a system to back up, other practices such as checking emails are reactive and require alert, well-trained staff to avoid costly mistakes. To help protect against cyber incidents, Australian SMBs need to accurately assess their level of cyber security understanding which will inform better cyber security practices. The Survey shows that many SMBs are overconfident in their cyber security understanding which increases their risk of a cyber incident, while other SMBs are too modest in their understanding and actually have better cyber security practices than they believed.

The Survey also revealed, and in some cases reaffirmed, the following critical insights about how the ACSC should deliver technical guidance to support Australian businesses:

- Technical advice must be prioritised so that Australian SMBs know which cyber security practices to implement first for best results.
- Guidance for Australian SMBs must be comprised of effective, low cost tips (in both time and money) that are easy to implement. Low cost tips will encourage uptake of guidance by SMBs, serving to maximise impact. This is why the ACSC focusses on effective, free, easy to implement DIY solutions.
- Plain language advice and explanations of technical terms, such as those provided in the ACSC's *Step-by-Step Guides* and *Quick Wins* for small businesses series, must be retained to improve comprehension and retention for SMBs.
- Cyber security guidance must also provide options that make it easier for time poor SMBs to stay on top of things, for example guidance that covers automating updates and backups, or setting calendar reminders for regular cyber security tasks. This will ensure cyber security practices are both implemented and maintained over time.
- The use of case studies in technical advice provides both tangible and relatable examples that show SMBs specific consequences of cyber incidents, outlines how SMBs recovered, and demonstrates preventative steps that can be taken to prevent future cyber incidents. Case studies should be used in cyber security advice because it will help Australian SMBs to better assess cyber risks and prioritise cyber security practices.