

# 2019 UNISYS SECURITY INDEX™

AUSTRALIA REPORT

**UNISYS** | Securing Your  
Tomorrow®

## Australia Summary

The 2019 Unisys Security Index™ surveyed more than 1,000 consumers in Australia, as part of an international study of more than 13,000 people across 13 countries, to gauge the public's concern about various security issues and how they change over time.

The Unisys Security Index for Australia – the overall measure of security concerns of the Australian public - is 155 out of 300, up from 151 in 2018 and continues a period of elevated concern over the last three years. This is lower than the global average of 175, and while it is only the eighth highest level of concern of the 13 countries surveyed, it is the second highest of the Western economies included in the survey and 16 points above neighbouring New Zealand.

The top three security concerns for Australians relate to data theft. More than half of adult Australians are seriously concerned about unauthorised access to their personal data (57%), bankcard fraud (56%) and computer hacking or viruses (54%).

For many Australians, the high concern about data security is based on experience. Nearly a third (29%) report they have suffered a data breach in the last year. The most common forms being email hacking, suspicious behaviour in their bank account and credit card details stolen.

But consumers are fighting back: many Australians have taken action against the organisations they hold responsible for not protecting their data against data breaches. Fifteen percent of those who suffered a data breach say they stopped dealing with the relevant organisation, 12% publicly exposed the issue via social media, 12% changed from paper statements and bills to electronic formats and 10% pursued legal action. Such action can impact an organisation's bottom line through customer loss, legal action or reputation damage.

When attending large events such as sports matches or music festivals Australians are equally fearful of data theft and physical attacks. Forty-three percent of Australian say they are seriously concerned about a criminal attack causing physical harm. Similarly, when using public Wi-Fi at the event 43% are seriously concerned about someone stealing their personal data from their mobile device and the same amount are concerned about someone stealing their credit card data.

This is impacting Australians' behaviour in relation to large public events. Three in 10 (30%) say they now think twice about attending large events and 19% have changed plans to attend certain events or certain locations. A quarter (23%) still attend large events but will take extra precautions to secure mobile devices and wallets. Just one in 10 Australians say their behaviours and decisions about attending events remain unchanged.

Given the high concern around the security of their personal information, Australians are discerning when it comes to data collection and sharing by organisations. Forty-one percent support the government collecting information to identify who is in the vicinity of a disaster, while only 10% support an employer monitoring an employee's location during the work day. And while two thirds support the police sharing information with other law enforcement agencies to solve a crime (66% support sharing with agencies in Australia, 65% support sharing with international agencies), only 16% are happy with banks sharing data with other financial service providers to provide a central point of contact for multiple services. More than half (57%) of Australians support doctors sharing an individual's healthcare history with other healthcare providers for a complete view of their health.

In today's hyper-connected world – for both individuals and organisations – Australians are wary of listening technology in smart devices such as smart watches and smart speakers. Forty-one percent of Australian smart device owners say they have received social media posts and ads about a topic they had recently talked about aloud, and two in three people in this group say they it concerns them.

## Global Summary

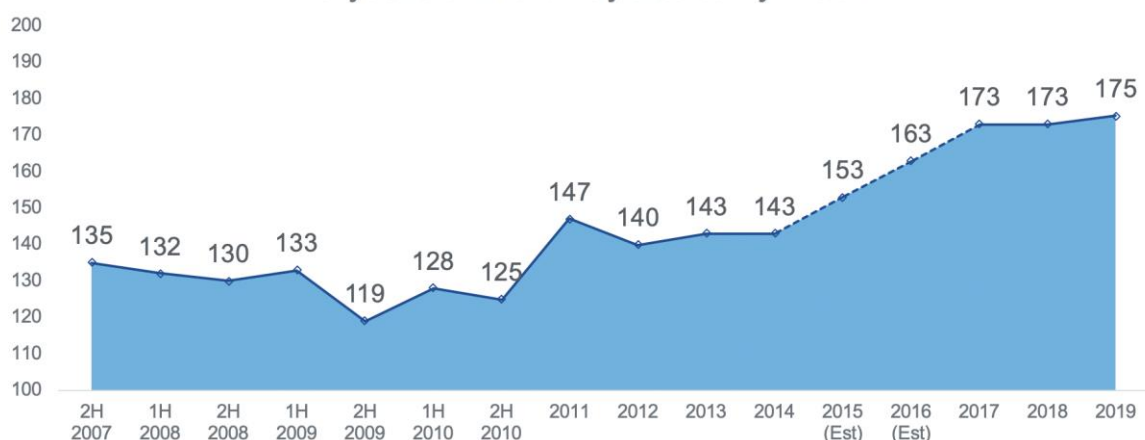
The Unisys Security Index has tracked security concerns around the globe for more than a decade and found those concerns to grow significantly over the past five years. This year, the global level of security concern was measured at its highest level since the survey began in 2007.

The 2019 Unisys Security Index stands at 175 (out of 300) globally, a two point increase since 2018. For the third consecutive year, Identity Theft and Bankcard Fraud continue to be the two most pressing concerns worldwide. Identity Theft continues to rank at the top out of the eight security threats measured by the index, with more than two thirds of those surveyed (69%) seriously concerned – exceeding reported concern related to National Security threats like war or terrorism and natural disasters. Bankcard Fraud also remains one of the top two security concerns globally, with two thirds (66%) of consumers seriously concerned about it.

Increasing internet security concerns are largely behind the rise in this year's Unisys Security Index. Nearly two thirds (63%) of consumers report they are seriously concerned about the threat of Viruses/Hacking with more than half (57%) seriously concerned about Online Shopping and Banking.

In general, consumers in developing countries<sup>1</sup> registered higher levels of concern than those in developed countries. Consumers in the Philippines reported the highest level of security concern of the 13 countries surveyed, and consumers in the Netherlands registered the lowest level – although their concern is rising. Younger respondents and those with lower incomes have higher security concerns in general.

13 years of the Unisys Security Index



The survey expanded its enquiry this year to include a look at the level of concern consumers register when they gather in large numbers at events such as the World Cup or large musical festivals. Following large public attacks around the world in the last year, the survey found that global security concern is high among consumers about attending these types of events.

Interestingly, consumers reported they are as fearful of having data stolen at large events as they are of being physically harmed. While 57% of respondents in the 13 countries surveyed registered serious concern (extremely/very concerned) about falling victim to a physical attack at a large event, the same percentage registered serious concern about having their personal data stolen when using public Wi-Fi at these events, and 59% were seriously concerned about someone stealing their credit card data.

Consequently, about a quarter of respondents (28%) have changed their plans to attend certain large-scale events and nearly four in 10 (39%) said they would “think twice” about attending. A quarter of those who have not changed their plans report they will take extra precautions about securing mobile devices and wallets.

<sup>1</sup> The Unisys Security Index defines a “developed” country as one in which the gross domestic product per capita is measured at \$12,000 or more.



# The Unisys Security Index: 13 Years and Counting

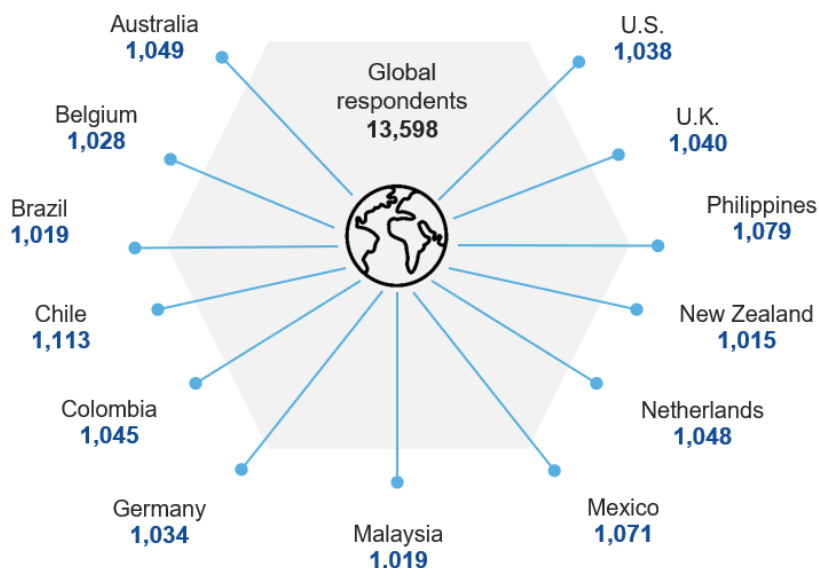
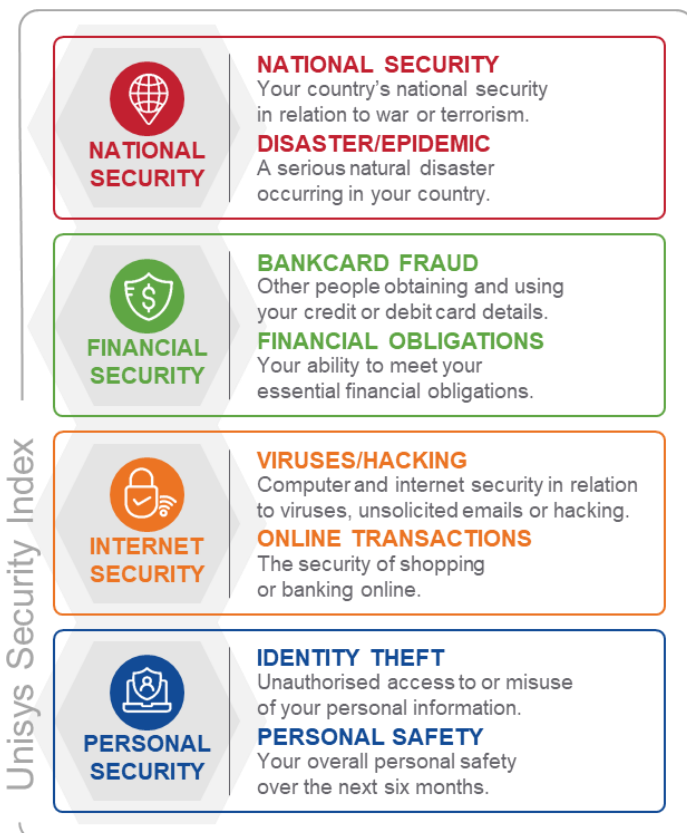
Unisys Corporation (NYSE: UIS) launched the Unisys Security Index – the longest-running snapshot of consumer security concerns conducted globally – in 2007 to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300<sup>2</sup> that measures consumer attitudes over time across eight areas of security in four categories:

The 2019 Unisys Security Index is based on national surveys of representative samples of at least 1,000 adult residents aged 18-64 years of age in each of the 13 countries surveyed, 13,598 in total. Interviews were conducted online 27 February–22 March, 2019. An additional question about security concerns at mass events was conducted 3 April–12 April, 2019 in some countries.

In all countries, the sample is weighted to national demographic characteristics such as gender, age and region.

Global security indices are unweighted averages of the 13 countries' respective security indices. The margin of error is +/-3.1% per country at 95% confidence level and +/-0.9% for the global results.

The 2019 Unisys Security Index survey was conducted by Reputation Leaders, a global thought leadership consultancy delivering compelling research that causes people to think about brands differently.



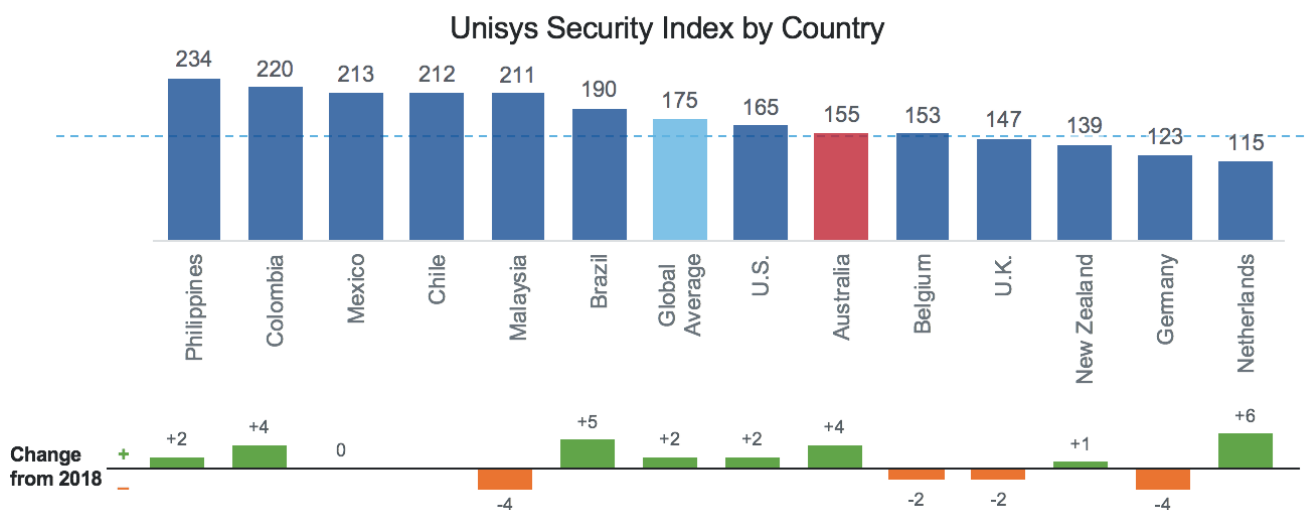
<sup>2</sup> The survey ranks concerns from zero to 300. One hundred means "somewhat concerned," 200 means "very concerned" and 300 means "seriously concerned."

## Key Findings: Australia

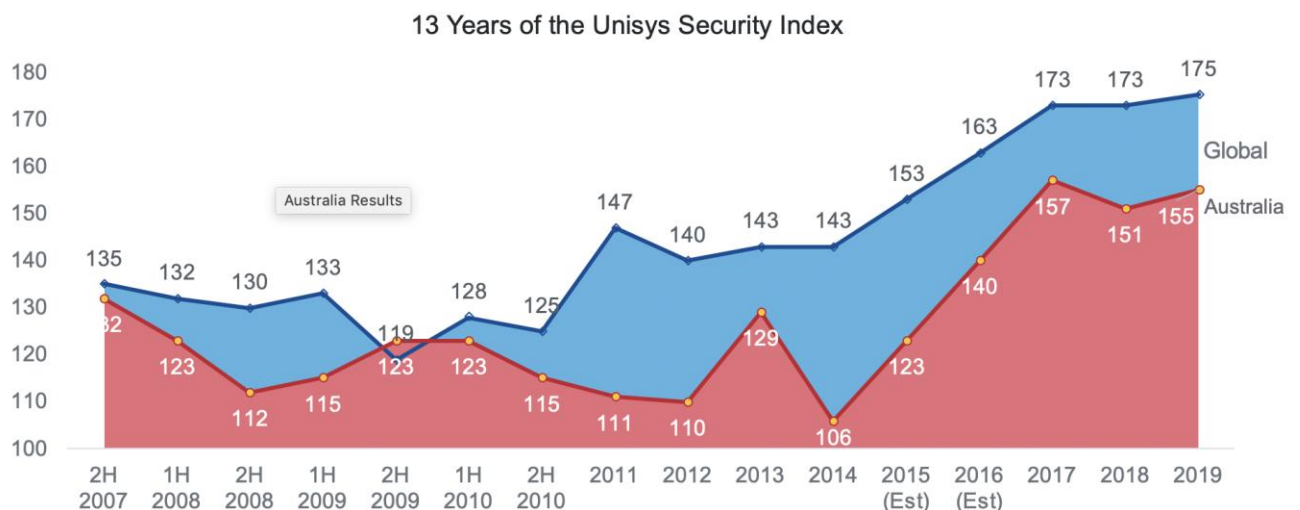
The Unisys Security Index for Australia – the overall measure of security concerns of the Australian public - is 155 out of 300, up from 151 in 2018 and continues a period of elevated concern over the last three years.

This is lower than the global average of 175, and while it is only the eighth highest level of concern of the 13 countries surveyed, it is the second highest of the Western economies included in the survey and 16 points above neighbouring New Zealand.

In Australia, the level of concern varies by gender, age and geography. In 2019 women are more concerned than men (the Unisys Security Index for females is 161 vs 150 for males). Younger Australians aged 28-24 years are the most concerned age group and the level of concern drops until retirement age. Queenslanders have the highest level of overall concern with a Unisys Security Index of 162 – seven points above the national score, and Northern Territorians have the lowest level of concern at 125 – thirty points below the national score.



Australia continues the higher level of security concern since 2017's peak of 157.





# 2019 Unisys Security Index™

## Consumers' security concerns Australia

### SECURITY CONCERNS AT LARGE EVENTS

**DATA** **15%**  
of Aussies stopped  
dealing with an  
organisation after  
they suffered a  
**DATA BREACH** in  
the last year.

**THINK TWICE**  
**38%**   
say there is no acceptable  
situation for organisations  
to collect personal info  
from **SOCIAL MEDIA** or  
**WEARABLE DEVICES**.



#### PERSONAL

Aussies are more  
concerned about  
**IDENTITY THEFT** than  
physical risks of  
**PERSONAL SECURITY** or  
**NATURAL DISASTERS**.



#### INTERNET

**54%**  
are seriously concerned  
about the threat of  
**VIRUSES/ HACKING**.



#### NATIONAL

**HALF**  
are seriously concerned  
about **WAR** or **TERRORISM**.



#### FINANCIAL

**56%**  
**FINANCIAL SECURITY** continues to  
be a top area of concern, with 56%  
of Aussies seriously concerned  
about **BANKCARD FRAUD**.

*In 2019, global security concern was  
measured at 175, indicating serious  
concern and the highest level in 13  
years of the Unisys Security Index™.*

The Unisys Security Index™ is a global study that gauges the attitudes of consumers on a wide range of issues related to national, personal, financial and Internet security. The study polled nearly 13,600 adults in 13 countries February 27-March 22, 2019.

Join the conversation #Unisys #SecurityIndex

[unisyssecurityindex.com](https://unisyssecurityindex.com)

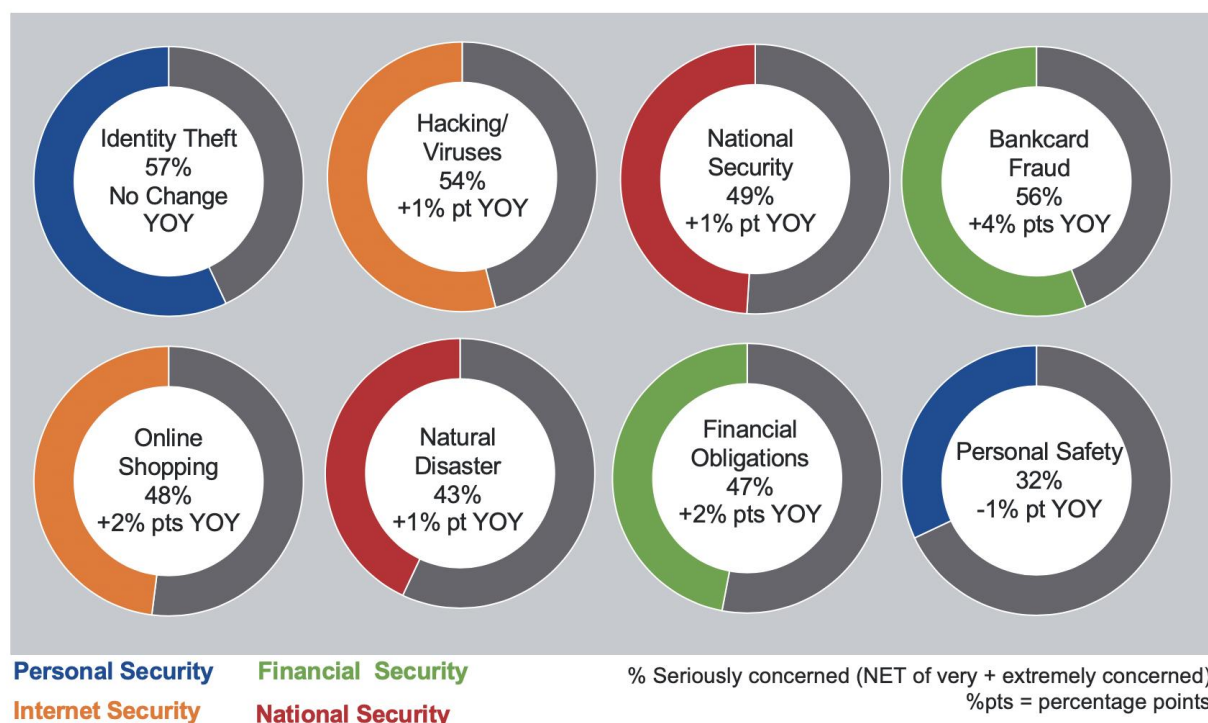


## Data Security Tops Australians' Security Concerns

The top three security concerns for Australians relate to data theft. More than half of adult Australians are seriously concerned about unauthorised access to their personal data (57%), bankcard fraud (56%) and computer hacking or viruses (54%). The biggest change from 2018 is growing concern in bankcard fraud which increased from 52% last year.

Meanwhile, approximately half of the population (49%) are concerned about national security in relation to the threat of war or terrorism, remaining steady with the previous year.

Other types of physical threats concern Australians the least with 43% concerned about natural disasters and only 32% concerned about personal safety.

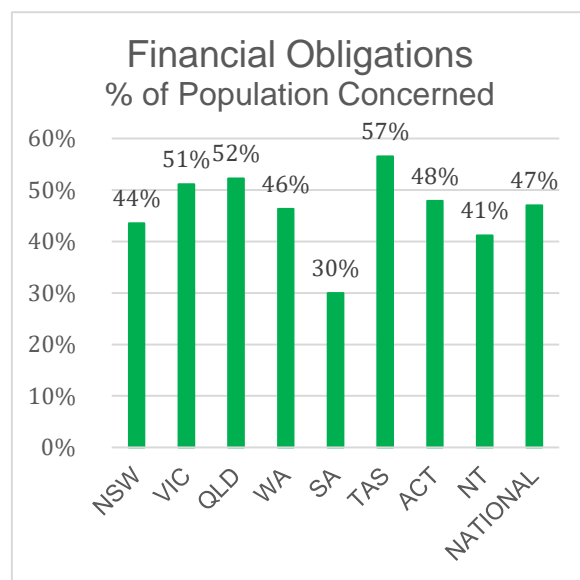
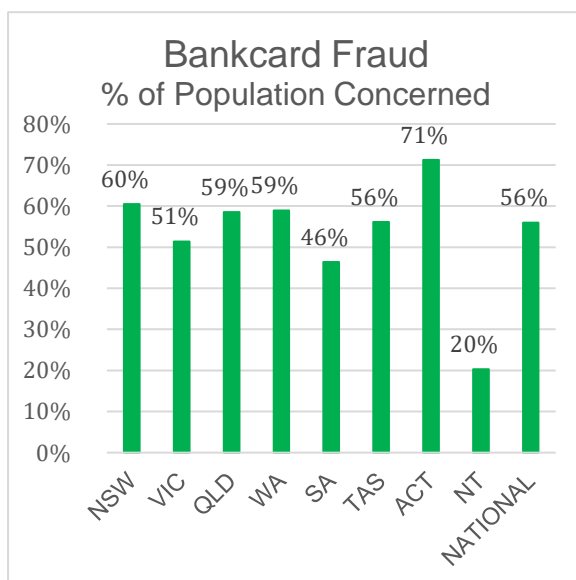
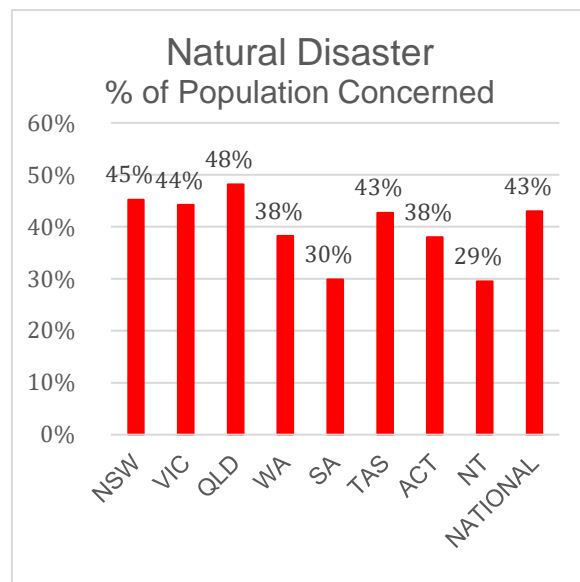
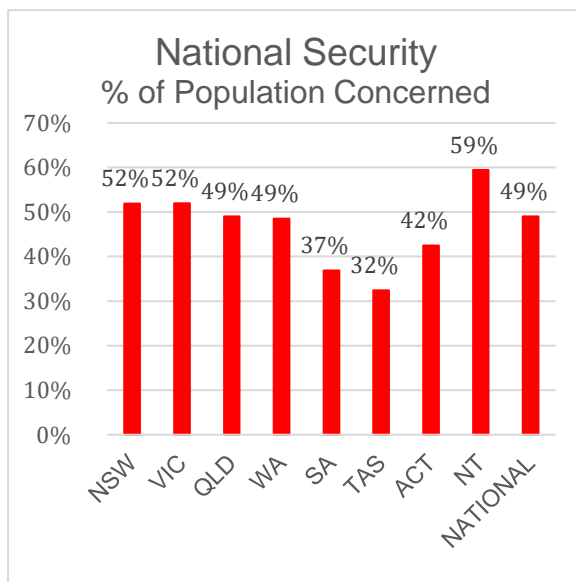
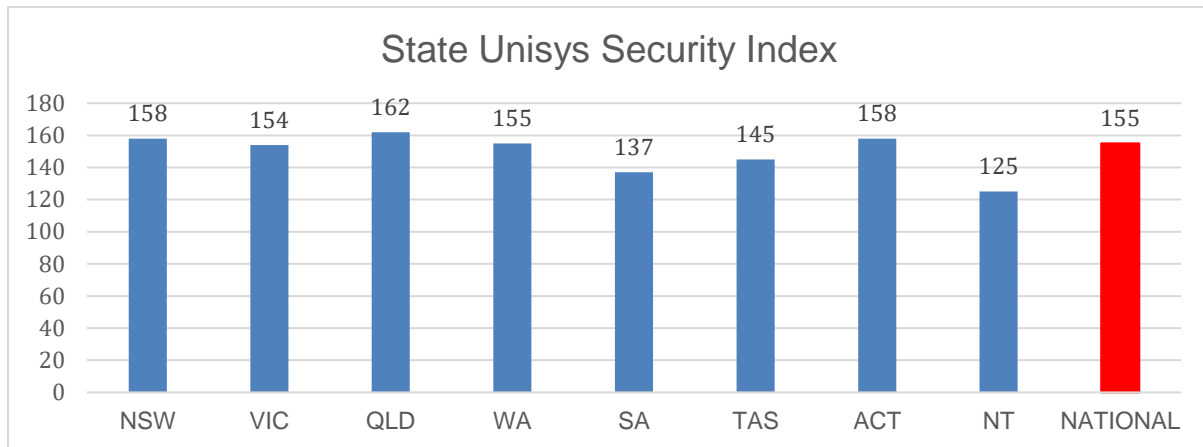


Again, there are demographic differences. Australian females are more concerned than males about natural disasters such as earthquakes, floods or epidemics with 48% of females compared to 39% of males concerned about this issue. Females are also more concerned about the threat to national security in relation to war or terrorism (52% of females, compared to 47% of males concerned) and the ability to meet financial obligations (49% of females, compared to 44% of males).

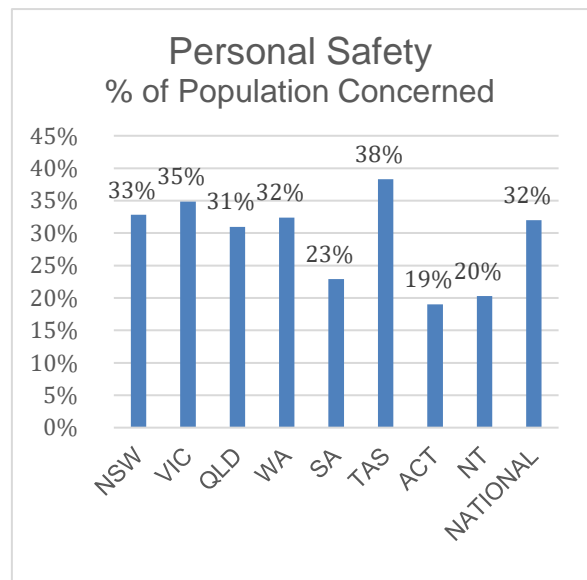
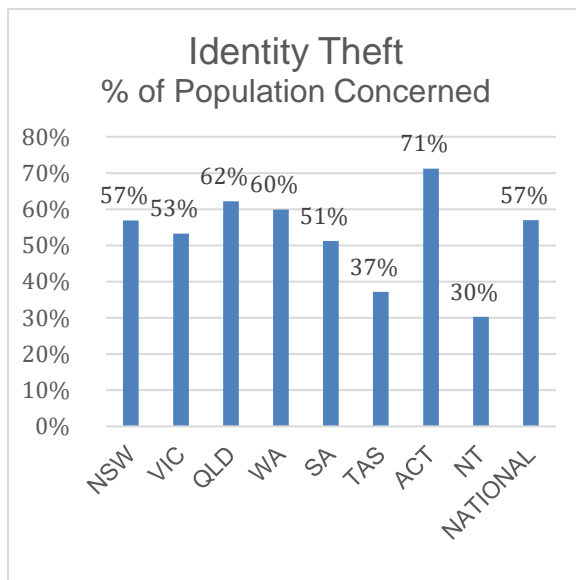
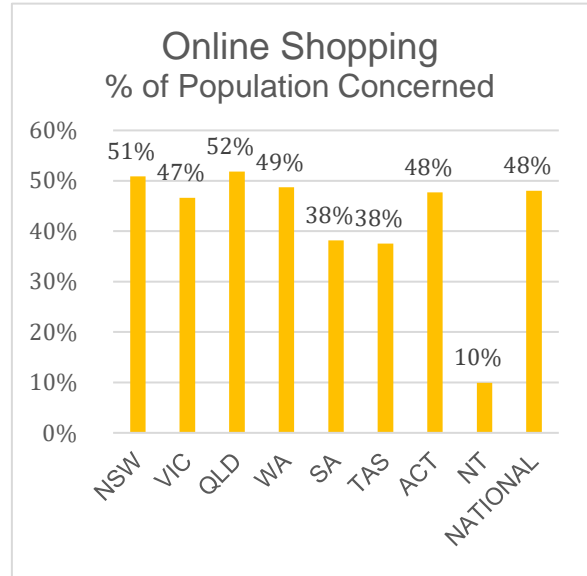
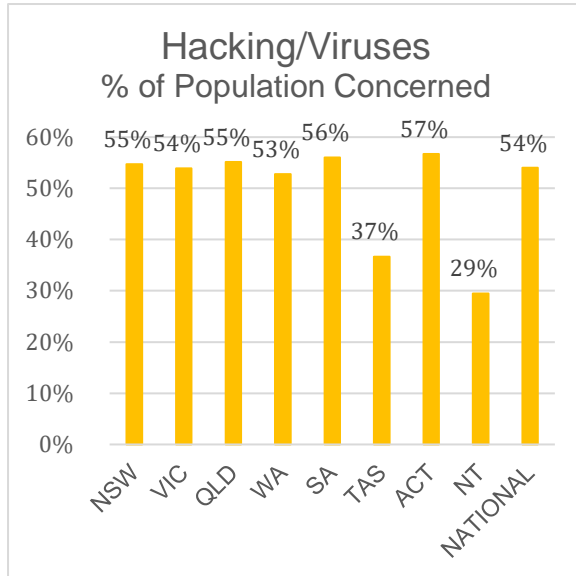
People living in Queensland, the Australian Capital Territory (ACT) and New South Wales (NSW) are more concerned than those who live in the Northern Territory, South Australia and Tasmania. In particular, Australians in the ACT have the highest level of concern for theft of credit card data and identity theft. Northern Territorians have the nation's highest level of concern for national security in relation to war or terrorism (59% of people concerned about this issue) but have low levels of concern for all other security issues.

Those living in smaller towns or rural areas tend to have a higher level of concern than those in cities with populations of at least 150,000, and much higher than those in state or national capital cities – particularly for national security in relation to war or terrorism, natural disasters and the ability to meet financial obligations.

## State vs State Comparisons







## Additional Research for 2019:

### Deep Dive into Today's Security Concerns for Australians

As part of the Unisys Security Index study, we also poll consumers on security issues they face in the current year and local market. In 2019 in Australia we looked at:

1. Security concerns around large events such as major sporting matches or music festivals.
2. The type of data breaches Australians suffered over the last year and what action they took.
3. How Australians feel about government and commercial organisations collecting, analysing and sharing personal data.
4. Whether they had experienced smart speaker technology unexpectedly listening to a conversation or monitoring their activity in today's hyper-connected world.

### 1. Security Concerns At Large Events

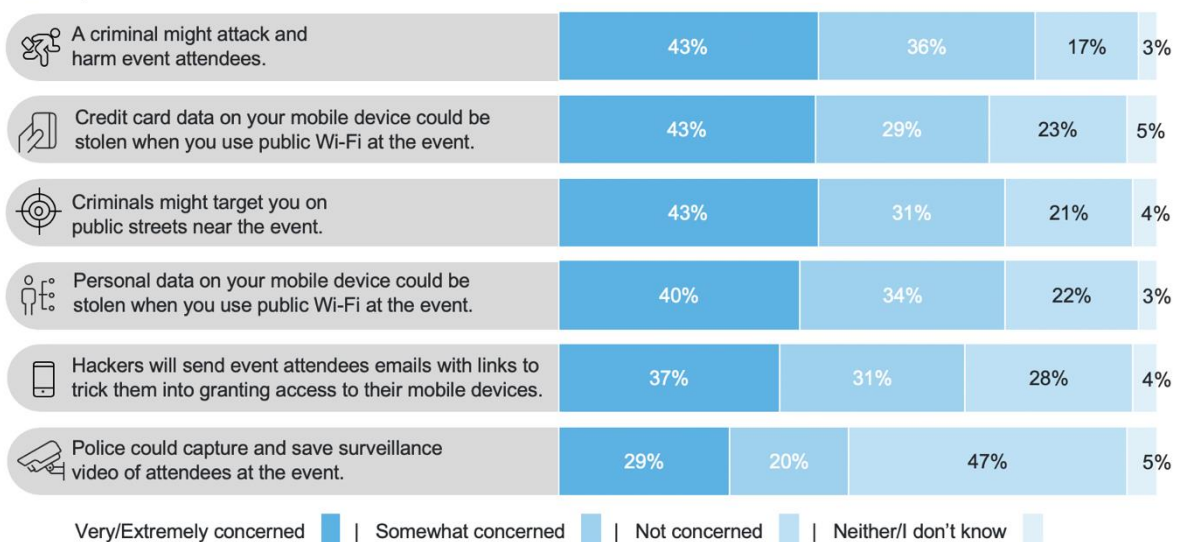
Reflecting Australians' concerns around data theft, Aussies are equally concerned about cyber and physical threats at large-scale events such as sporting events or music festivals.

Forty-three percent are seriously concerned about someone stealing their personal data from their mobile device and the same percentage is concerned about someone stealing their credit card data when using public Wi-Fi. Just one in five (21%) remain unconcerned about their personal data being compromised at a large public event.

Similarly 43% of Australians say they are seriously concerned about a criminal attack causing physical harm. This reflects ongoing reports of terror plots in Australia targeting places where crowds congregate such Melbourne's CBD at Christmas and ANZAC Day services in Australia and Gallipoli, as well attacks overseas – particularly in the UK. (NB the survey was fielded before the Christchurch mosque attacks in neighbouring New Zealand).

Fewer people are concerned about being physically attacked near an event (40%) or event attendees being targeted by hackers (37%). Only 29% of Australians say they are concerned that police could capture and save the surveillance video of attendees at the event.

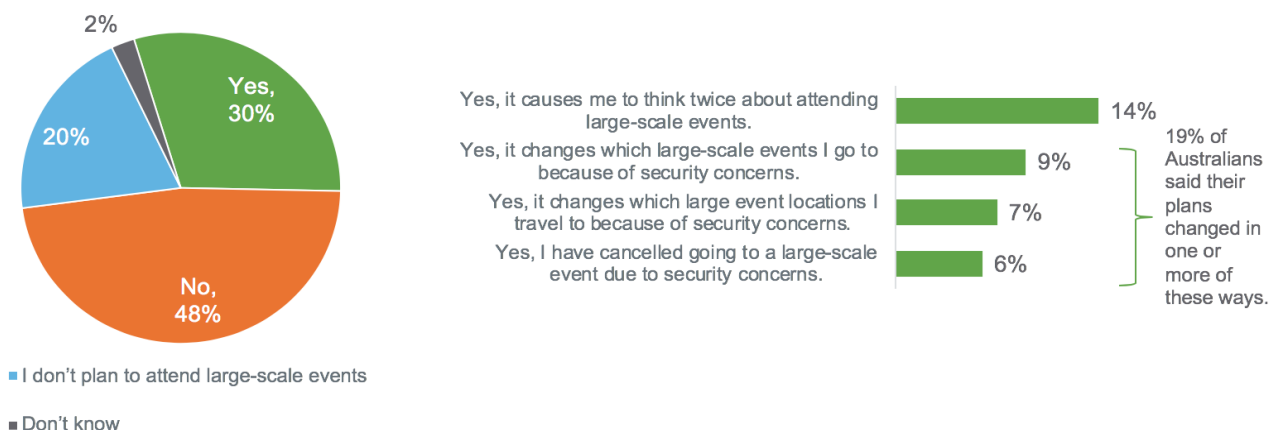
When travelling to a large-scale event such as a World Cup or a large music festival, how concerned are you about the following security issues?



These concerns are having an impact on Australian's decisions and behaviours about attending large-scale events: 30% of Australians say they now think twice about attending such events and 19% have changed their plans to attend certain events due to the possibility of having their data stolen or being subject to physical harm.

While almost half (48%) of respondents report security concerns have not impacted their plans to attend large events, 23% say they now take extra precautions to secure their mobile devices and wallets and 17% say they now keep on guard for suspicious or threatening behaviour.

Has the possibility of having your data stolen or being subject to physical harm a large-scale event such as a World Cup or a large music festival caused you to think twice about attending?



Rick Mayhew, vice president and general manager, Unisys Asia Pacific explains: "The research findings highlight the convergence of physical and cyber threats in our everyday lives. Australians are aware of the various potential threats at big events – the good news is that awareness is the first step to protection. Australians are proactively protecting themselves by taking precautions to protect their information, being vigilant about what is happening around them and, in some cases, choosing not to attend events or locations where they feel unsafe. However, the temptation is to jump on any free Wi-Fi to avoid racking up mobile data costs. Always assume public Wi-Fi is unsecure and be cautious. If the device is used for work, employers should mandate use of a Virtual Private Network (VPN), regardless of whether the device is provided by the employer or employee."



## 10 Tips to Stay Safe at Large Events

Salvatore Sinno, global chief security architect at Unisys, provides the following list of simple steps people can take to stay safe and secure at major sporting events, concerts and festivals:

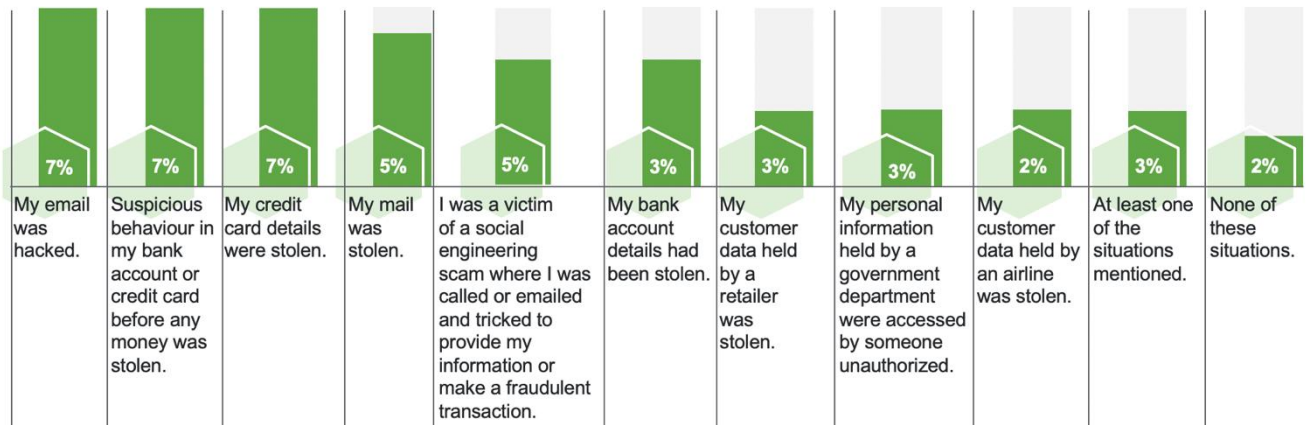
1. **Only buy event tickets from official channels or websites you trust.** Make sure the website you're using to buy tickets shows the secure padlock icon in the browser and the address begins "https://". And if ticket prices look too good to be true, they probably are.
2. **Plan ahead and check local authorities' alerts.** Sign up for any travel or news alerts provided or recommended by the event organisers to receive updates on traffic or news of any potential disturbances on event day.
3. **If you're going to a crowded event alone, let someone know.** Make sure your friends or family know where you're going, when you plan to arrive and when you're expected to return.
4. **Travel light.** There's no need to take everything you own to a festival. Leave the valuables at home and travel light, with just the essentials – in your pockets if possible.
5. **As soon as you get to the event, survey your surroundings.** Make sure you know where the exits are and agree on a meeting place with your friends in case you should get separated from your group. Know where stewards and information points are so you can speak to someone if you need to.
6. **Update your mobile device and avoid unsecured Wi-Fi networks.** Make sure your phone is updated with the latest software, so it's as secure as it can be. And only use password protected Wi-Fi. Unprotected Wi-Fi networks could give hackers access to personal or financial data on your phone.
7. **Don't make electronic transactions with unofficial event vendors.** Be careful with your contactless cards or making mobile transactions, particularly outside event venues. Unscrupulous traders could be gathering your financial data to use or sell to other criminals.
8. **Be vigilant for suspicious activity at an event.** Don't be afraid to report something you think is unusual, such as unattended baggage or people behaving in a suspicious or threatening way.
9. **Keep your phone charged in case of emergencies.** If possible, take a battery charger pack with you to ensure your phone is always available when you need it.
10. **In an emergency, stay calm and move to the edges of crowds.** Try to leave the area quickly and calmly. If you need to, get away from the incident quickly, hide yourself if need be, call 000 (or 112 from your mobile) when you can, and then let your family know you are safe.

## 2. Australians Hit Back After Data Breaches

Nearly one third (29%) of Australians say they have experienced a data breach in the last year. This is similar to the rate reported in New Zealand (28%) and lower than in Malaysia (46%) or the Philippines (36%).

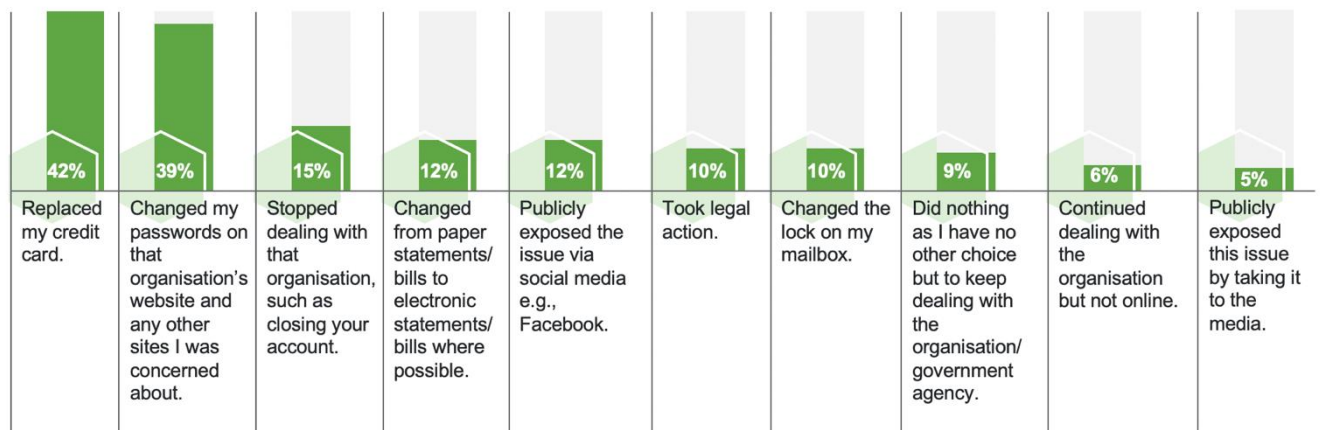
The most common breaches experienced in Australia are email hacking (7%), suspicious bank account behaviour (7%) and stolen credit card details (7%).

Have you suffered any of the following data breaches or events in the last 12 months?



Almost all Australians take action after suffering a data breach. Of those affected, 15% will stop dealing with the relevant organisation altogether, and 10% have pursued legal action.

If you were in any of the scenarios described in the previous question, what action did you take?



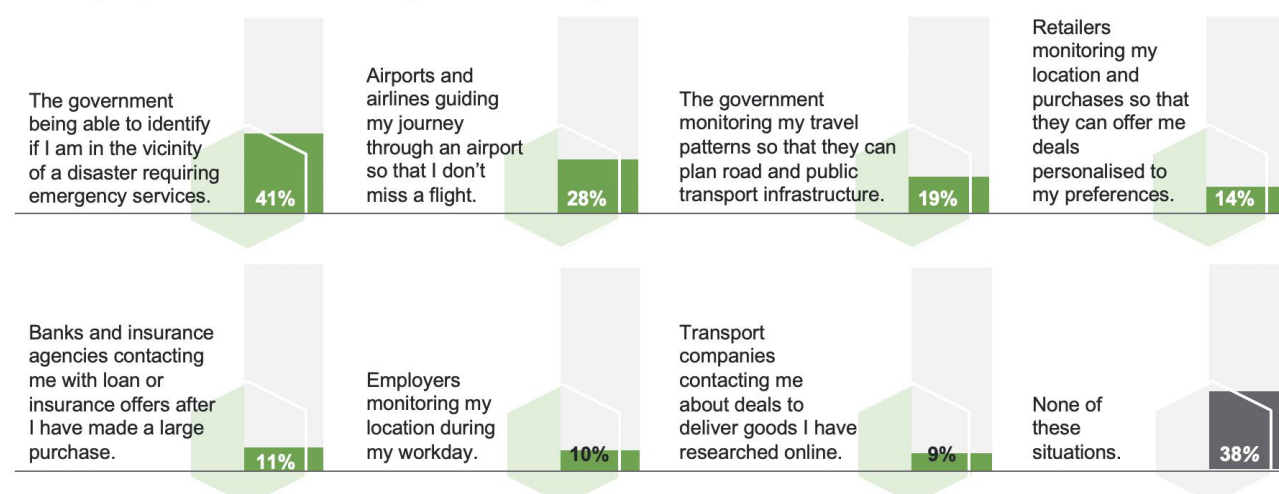
### 3. Support for Government and Commercial Organisations Collecting, Analysing and Sharing Personal Data Varies

Data analytics has been hailed by many as the “next big disruptor” across many industries for several years. But today’s hyper-connected world featuring wearable tech, social media, geolocation apps, smart devices and a “digital first” strategy by most governments and organisations to move their services online means that more information than ever about individuals is available for the taking.

However, Australians are discerning about which situations they deem acceptable for an organisation to collect data from social media, online purchases, smartphones and wearable devices. Four in ten Australians (41%) support the government collecting this information to identify who is in the vicinity of a disaster, yet only 19% support the government monitoring an individual’s travel patterns to plan road and public infrastructure. More than a quarter (28%) support airports and airlines collecting the information to efficiently guide a passenger’s journey through an airport, but only 10% support an employer doing the same to monitor an employee’s location during the work day.

More than a third of Australians (38%) say that there is no acceptable situation for collecting data from smartphones and wearable devices – the highest level of objection compared to the other three countries where this question was fielded: New Zealand (36%), the Philippines (20%) and Malaysia (14%).

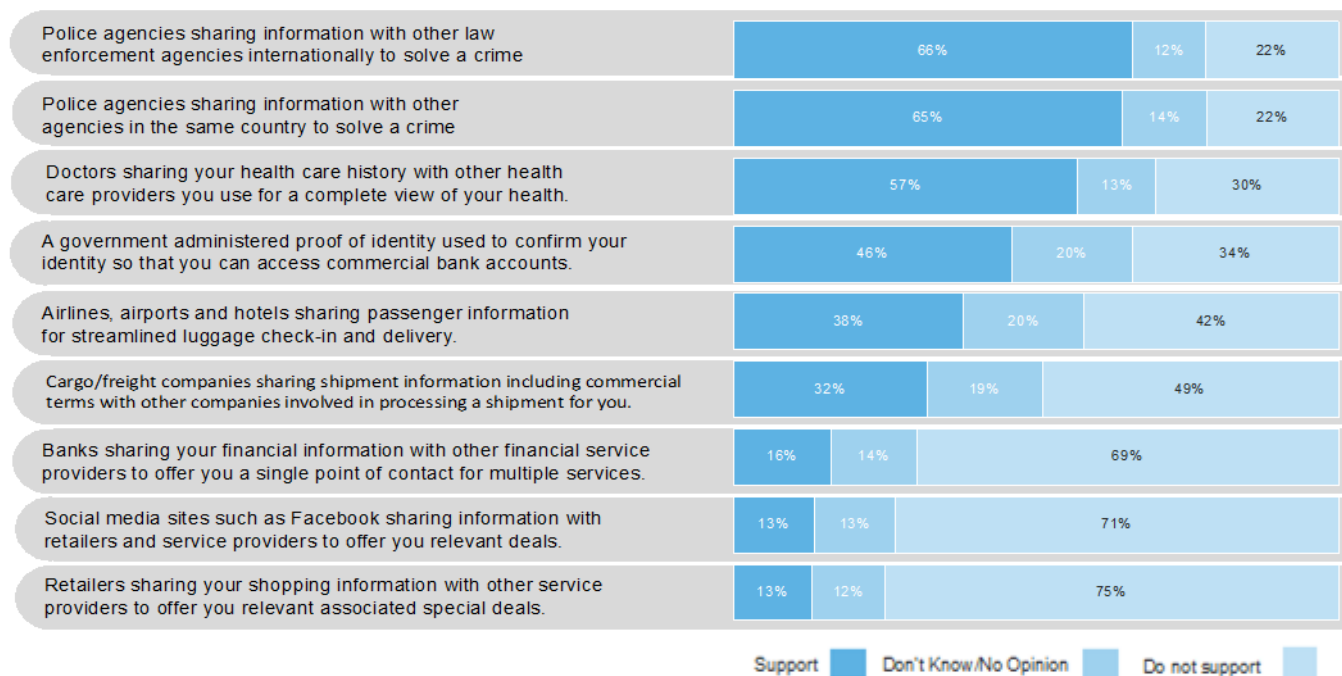
In which of the following situations, if any, do you support information being collected from any of your social media, online purchases, smartphone or wearable devices?



Similarly, the Australian public’s support varies for organisations sharing an individual’s personal information with other organisations. The highest support is for police sharing information with other law enforcement agencies within Australia (66%) or internationally (67%) to solve a crime. There is also strong support (57%) for doctors sharing a patient’s healthcare history with other healthcare providers the patient uses for a complete view of the individual’s health. Almost half of Aussies (46%) support a government-administered proof-of-identity used to confirm a citizen’s identity to access commercial services such as a bank account. However, only 16% support banks sharing a customer’s financial data with another financial service provider to offer a single point of contact for multiple services.



## In which of the following scenarios do you support an organisation sharing your personal information?



For all scenarios, the top two reasons given by Australians for not supporting their data being shared is that they want control over exactly who has access to their personal information, and they don't want the other organisation to have access to their data. This marks a concern around privacy, rather than the ability of an organisation to secure the data.

"There is strong support, and probably an expectation, from the Australian public to allow police to share information with other agencies to help them 'join the dots' to solve or prevent crimes. This could mean preventing attacks at events or enabling earlier intervention by welfare agencies to prevent child or spousal abuse. But trust is fragile, and to retain this high level of public trust in Australian law enforcement, any information sharing must be done in a secure fashion where only the right people from appropriate organisations can access such sensitive information," Mr Mayhew cautions.

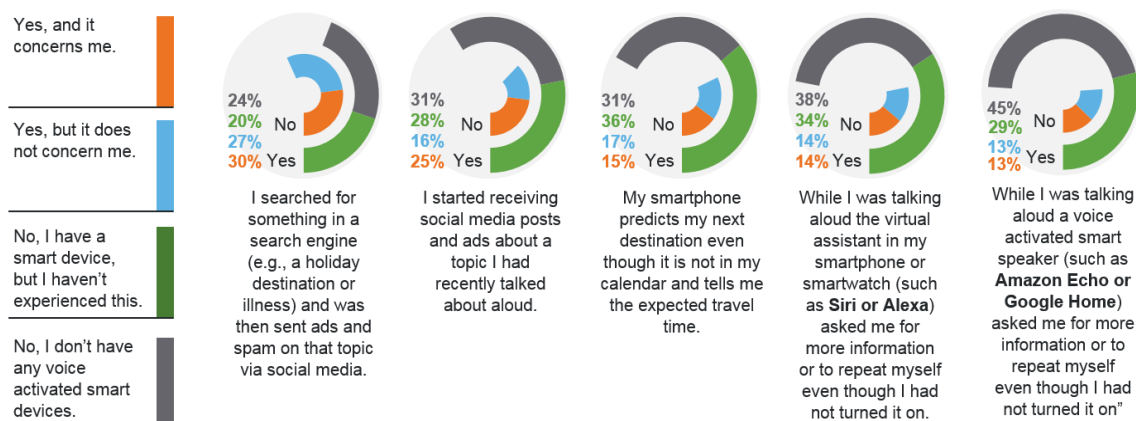
## 4. Aussies Not Comfortable with Smart Listening Devices in Today's Hyper-Connected World

Today we live in a hyper-connected world – for both individuals and organisations – from smart phones and smart watches through to smart homes and digital assistants. A growing component in this is the rise of voice-activated command driven digital assistants either embedded in smart phones and smart watches or in purpose-built devices such as smart speakers. The Amazon Echo and Google Home are the dominant brands in the US and Europe, while Chinese brands of Alibaba, Xiaomi and Baidu are popular across Asia.

The first devices were introduced just five years ago, but the global smart speaker market is expected to overtake tablets by 2021<sup>3</sup>. However, as more people have embraced technology, so has the speculation that these devices listen in or monitor conversations even when they haven't been activated. This section of the study explores the Australian public's perception of how emerging technology based on Internet of Things (IoT) and artificial intelligence (AI) might impact our privacy by monitoring our conversations and activity. It asks Australians if they think this is happening, and if so, are they concerned about it: They believe it is and they are concerned.

Forty-one percent of Australian smart device owners say they started receiving social media posts and ads about a topic they had recently talked about aloud, and almost two thirds of this group say it concerns them. Just over a quarter (26%) report that while talking aloud the virtual assistant in their smartphone or smart watch had asked them for more information or to repeat themselves even though they had not turned it on. Similarly 23% say that while talking aloud, a voice activated smart speaker had asked them for more information or to repeat themselves even though they had not turned it on. In both cases, approximately half of people who experienced this say that it concerns them.

Have you experienced any of the following?



3 – Canalsys Media release: [Global Smart Speaker Installed Base to Top 200 million by the end of 2019](#) (April 2019)

## The Unisys Perspective

### CONSUMER CONCERN IS GROWING ACROSS THE BOARD

Given the political turmoil of recent years, combined with reports of incidents of physical violence and a seemingly endless series of cyber attacks on both governments and private enterprises, it comes as no surprise that the 2019 Unisys Security Index reports the highest-ever level of global security concerns among individuals in the years that the survey has been conducted. "There are security concerns in every sector of the world, in every industry, in everything that you do – and it's overwhelming," says Chris Kloes, vice president of Unisys Security Solutions.

The continued growth in concern may be at least partially a product of greater awareness on the part of consumers of threats that exist both online and off. This growing recognition has caused consumers to lose trust in organisations that handle their personal data.

"Society is starting to wake up now and say, 'My personal information really is important, and I'm learning that people can do really bad things with it. For example, I've been alerted by the Government Tax Department that my social security number was being used to impersonate me. Until they contacted me, I had no idea this was going on. This seriously affects me directly,' "says Jeff Livingstone, Unisys Vice President and Global Head of Life Sciences & Healthcare.

"In the world of healthcare, public concerns related to personal data security and privacy are increasing rapidly," Livingstone continued. "And it's largely because, up until two years ago, highly-publicised attacks and massive releases of private information were not as proliferative as they are today. Another contributing factor is that financial and billing processes in healthcare organisations are highly "laggy". Often there is substantial time between a medical service and the patient's receipt of the actual bill. This gives hackers a large window in which they can do terrible things. Healthcare data can be used to establish entire online personas, and for this reason is much more valuable to cybercriminals than classic financial information. The value of healthcare information on the black market is exponentially increasing. Hence all these factors have come together in sort of a perfect storm, aimed directly at the healthcare consumer."

Maria Allen, vice president and global head of Financial Services at Unisys, points to a similar trend at financial institutions. "There's much more information out there, and the banks have become more open to digital solutions and automation, all of which is bringing some additional focus and additional concerns on the part of consumers about all aspects of security," Allen said.

Ironically, the trend is exacerbated by attempts by healthcare providers and those in other industries to improve service to their clients through technology, Kloes notes. "Many organisations are now using technology to put more decision-making power in the hands of the consumer with things like new apps and home-based devices," he said. "All of those things now create a risk for which neither the consumer nor the service provider is fully prepared. The consumer will make the incorrect assumption that the apps on his or her phone have been vetted and are secure, and there will be an inevitable collision between the consumer's perception and the ability to serve that consumer from a cybersecurity perspective."



## **SECURITY CONCERNS EXTEND TO LEISURE ACTIVITIES LIKE ATTENDING LARGE-SCALE EVENTS**

Governments and private organisations have long been focused on ensuring the physical safety of attendees at global events such as the Olympic Games or the various World Cups. In recent years, however, several highly-publicised tragedies at concerts and other large gatherings have prompted concerns related to events that take place at a regional or local level. In addition, the 2019 Unisys Security Index results show that consumers are just as concerned about the security of their data at public events as they are about their physical security.

This raises the question of how government public safety agencies, event organisers and others address the broad array of concerns raised by consumers.

Mark Forman, Unisys vice president and global head of Public Sector, says some governments and enterprises are finding ways to proactively deal with new threats. “Proactive defence requires a combination of technology, education to increase cyber security awareness and to support the development of skilled cyber security professionals.”

## **IDENTITY THEFT CONTINUES TO BE VIEWED AS A HUGE THREAT**

Unisys chief information security officer Mathew Newfield notes that consumers’ growing dependence on online identities extends to nearly every aspect of their lives. “From my perspective, I see identity theft as encompassing a lot of other parts of the security conversation,” said Newfield. “I think there’s been an awakening in the world that if someone steals your identity, they’re getting to your bankcard, your finances, your tax returns, your online shopping and more. And when they start realising that someone can buy identities in bulk for less than a dollar apiece, I think people are getting scared.”

Newfield added that the consequences of identity theft can vary from country to country. “In 2018 the European Union adopted the General Data Protection Regulation (GDPR) to tighten rules about how companies harvest and manage data, with hefty penalties for violators. In Australia the Privacy Act regulates the handling of personal information about individuals. Under the Notifiable Data Breaches (NDB) scheme Australian Government agencies and the various organisations with obligations to secure personal information are mandated to notify individuals affected by data breaches that are likely to result in serious harm. Similarly in New Zealand the Privacy Act controls how organisations collect, use, disclose, store and give access to personal information, however currently it is not a mandatory requirement to report data breaches. In 2010 Malaysia introduced a comprehensive personal data protection legislation, the Personal Data Protection Act (PDPA), which came into force in 2013. However, like New Zealand there is no requirement under the PDPA for data users to notify authorities regarding data breaches in Malaysia.”

## **Conclusion**

Consumer concern continues to grow around the world, in all areas of security and across all sectors and industries. These concerns have profound implications for the companies and government agencies they rely upon to protect them and their data. These organisations must prioritise security to address these concerns, starting with a Zero Trust approach to identify all actors, systems and services operating within the enterprise.

## Calls to Action

So, what can businesses and governmental agencies that serve consumers do? Unisys believes there are tangible steps they can take.

### **1. *Continue to move toward adoption of a Zero Trust security model that assumes all network traffic is a potential threat.***

The continued increase in consumer concern about online security reflected in the 2019 Unisys Security Index underscores the continuing imperative to take all measures possible to assure clients that their data is protected when they work with an organisation.

Unisys recommends a five-step methodology as a roadmap for getting to a complete, start-to-finish Zero Trust implementation. The five steps to Zero Trust are:

- **Prioritise:** The Zero Trust journey starts with total ecosystem visibility, enabling organisations to understand their vulnerabilities and set priorities.
- **Protect:** Based on their priorities, organisations must first protect their most vulnerable people, devices and networks, and then extend protection to all.
- **Predict:** Organisations must get ahead of threats and strengthen their risk postures with AI-powered predictive threat prevention and objective, data-driven, cyber risk forecasts.
- **Isolate:** Organisations should isolate critical data and systems, preventing access from rogue users.
- **Remediate:** Unisys helps organisations minimise the operational impact of attacks by reducing their incident response time.

"IT decision-makers have long recognised that the network perimeter is indefensible in today's technology ecosystem," says Kloes. "Unisys Security Solutions addresses this by implementing a zero trust architecture that grows with today's organisations. Leveraging dynamic isolation™ capabilities to quickly isolate devices or users at the first sign of compromise, Unisys identifies, validates and secures trusted users, devices and data flows."

### **2. *Technology is important for addressing consumer security concerns, but people are important, too.***

The best security technology can go a long way toward analysing network activity and identifying security issues before they escalate. But even the best technology won't be effective without experts possessing the ability to interpret and act upon information received. Unisys recommends that organisations focus on both technology and people in order to meet the expectations of increasingly concerned customers.

"Security is a multi-dimensional discipline," says Forman. "Technology can do a lot in terms of assembly and analysis of information, but you need a way to engage the right people in using the insights. We see this, for example, with border security technology, which often is focused on data analysis but lacks the ability to communicate insights in a timely and useful manner needed to stop a threat. Unisys recognises that the last mile is the big gap in many of these tools that must be addressed."

### 3. *Address the risk associated with the growing number of devices in and around the enterprise and where employees are taking them.*

The results of the 2019 Unisys Security Index clearly illustrate the slowly disappearing line between physical and online security. And as mobile devices proliferate throughout the enterprise, employees are also taking them to physical locations where they may encounter a high amount of cyber risk. While many enterprises work hard to guarantee the physical safety of their people, the safety of their data may not be getting as much attention as it requires.

Programs in which employees were travelling to high-risk areas are issued temporary, prepaid burner devices are helpful in terms of allowing them to work more safely and without as much risk to the enterprise. Organisations also should provide clear guidance to their people on what to do and what not to do when operating in risky physical environments.

For more information on Unisys security offerings, visit: [unisys.com/security](https://unisys.com/security).

"A lot of companies are missing the opportunity to help their associates, employees and executives to work safely when they travel to areas where security concern is high," says Livingstone. "Companies should not only safeguard these employees' devices and data but also provide guidance such as, 'Do not go to specified risky areas, only accept rides in specified types of vehicles, do not get a first-floor hotel room and so on.'"

## About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most demanding businesses and governments on Earth. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing. For more information on how Unisys builds better outcomes securely for its clients across the Government, Financial Services and Commercial markets, visit [unisys.com](https://unisys.com).

## About the Unisys Security Index

Unisys has conducted the Unisys Security Index – the longest-running snapshot of consumer security concerns conducted globally – since 2007 to provide an ongoing, statistically-robust measure of concern about security. The index is a calculated score out of 300 covering changing consumer attitudes over time across eight areas of security in four categories: **National Security** including war or terrorism and natural disasters or epidemics; **Financial Security** spanning bankcard fraud and the ability to meet financial obligations; **Internet Security** concerns of viruses/hacking and online transactions; and **Personal Security** concerns around identity theft and personal safety. The 2019 Unisys Security Index is based on online surveys conducted 27 February–22 March, 2019 of nationally representative samples of at least 1,000 adults in each of the following countries: Australia, Belgium, Brazil, Chile, Colombia, Germany, Malaysia, Mexico, Netherlands, New Zealand, Philippines, the U.K. and the U.S. The margin of error at a country level is +/-3.1% at 95% confidence level, and +/-0.9% at a global level.

For more information on the 2019 Unisys Security Index for Australia visit [unisyssecurityindex.com.au](https://unisyssecurityindex.com.au) and for all 13 countries visit [unisyssecurityindex.com](https://unisyssecurityindex.com)