Data Report
February 2021

The State of Digital Trust

A snapshot of Australians' trust in an increasingly digital society

Okta Inc.
okta.com
press@okta.com

okta

Contents

Introduction: trust begins with feeling secure

The events of 2020 have exposed just how critical trust is for consumers and businesses alike. Organisations had to trust their employees to work from home, and consumers had to trust businesses with their information. As a society, we had to trust each other to make the right decisions around health and safety, trust the scientific community to create life-saving vaccines, and trust the government to support us during a time of global economic uncertainty and political upheaval.

All this comes amidst a backdrop of rising security concerns, highlighted by the Australian Federal Government releasing a new Cyber Security Strategy, announcing Australia's largest ever investment in cyber security and giving clear warnings of the increased risk of cyber attacks[i]. 2020 also saw a number of Australian organisations impacted by malicious cyber attacks[ii], along with rising data breach volumes and cyber-threat activity, opportunistic social engineering scams, rigorous regulatory enforcement of data protection legislation, and soaring privacy expectations among consumers.

At Okta, we wanted to know what trust looks like in this increasingly digital world, so we worked with YouGov to survey more than 1,000 Australian workers and 15,000 office workers in total around the world (US, UK, Netherlands, Italy, France, Sweden, Australia, Germany, Japan, and Spain). We set out to see how much we trust when we only engage online, if brands have done enough in the eyes of consumers to build trust, and what factors impact the way we interact with digital services.

We found that when it comes to building trust in Australia, consumers care most about the core competencies: service reliability, strong security, and good data handling practices. Survey respondents also made it clear that trust in their digital world directly impacts purchase decisions, and many will cut ties with brands they lose trust in.

[i] https://www.pm.gov.au/media/statement-malicious-cyber-activity-against-australian-networks
[ii] https://home.kpmg/au/en/home/insights/2020/08/cyber-security-2020.html

Key takeaways

Trust is fundamental to consumers: The events in 2020 led to trust becoming fundamental online, with 77% of Australians saying they would be unlikely to purchase from a company they didn't trust. Getting the basics right is most important, with 32% saying reliable service (such as ensuring items arrive on time and in good condition) gives them the most trust in a digital brand. Security was the second most important criteria, with 24% telling us that having secure log-in options and other measures in place would help to nurture trust.

Brand reputation impacts online shopping: Australians are taking brand reputation more seriously than ever when it comes to where they spend their money online. If they don't know if a website is legitimate (54%), have concerns about data breaches (49%), or the website requests too much personal information (44%), many would have serious reservations about purchasing goods and services online.

Data ethics plays a key role: The top two reasons Australians lose trust in a brand are 1) knowing they were intentionally misusing or selling personal data (44%) and 2) falling prey to a data breach (16%).

Government websites are most trusted: By far, the most trustworthy of all digital channels is government websites, according to 41% of Australian respondents. 14% said they don't trust any digital channels to safely handle their data.

Consumer loyalty is hard to gain and easy to lose: Brands must work hard to retain trust, and effective cybersecurity is key. 40% of Australians say they have lost faith in a company due to a data breach or security event. Following an event, nearly half said they would permanently stop using the company's services and 43% would change their user settings such as passwords and email addresses. A further 41% would delete their account altogether.

Australians have become more cautious: With the rise of cyber threats over the past year, 57% of Australians say they have become more cautious about providing personal information about themselves online. Working from home practices have also made respondents more wary of phishing emails (45%), data breaches (43%) and even AI-generated "deepfakes" used to spread false information (37%).

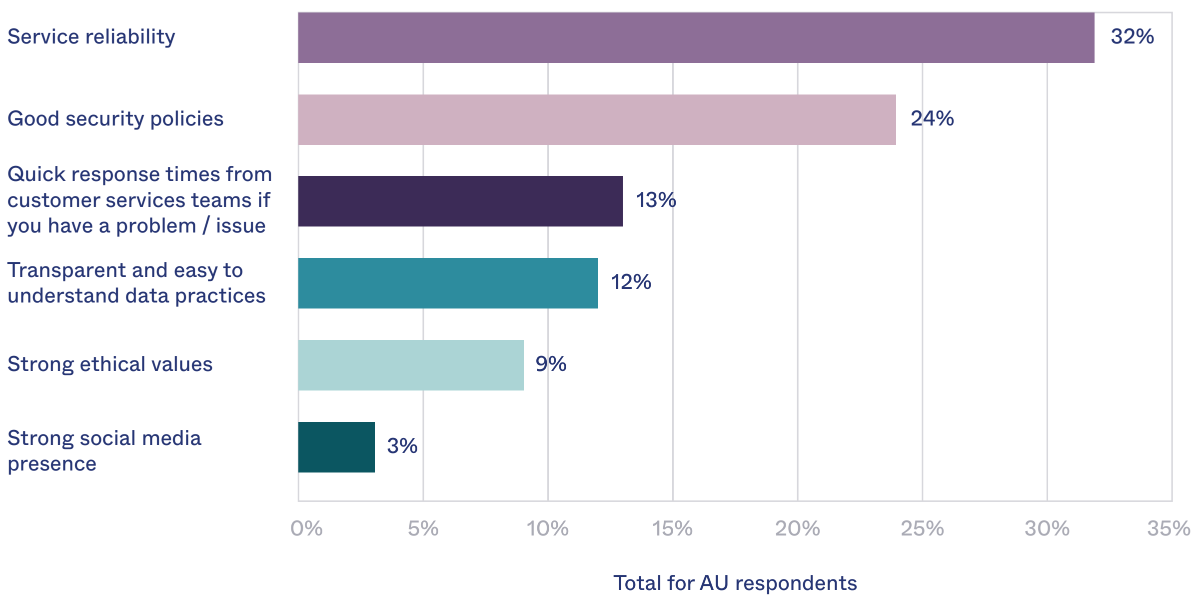
Media coverage is key in disseminating information about online threats: Australians have increased caution online during the pandemic for the most part due to media coverage about scams and cybersecurity threats (44%).

What makes consumers trust brands?

In 2020, as the world locked down and shifted to remote working, office workers spent a lot more time and money online. Australia's ecommerce growth was the highest across the globe by the final half of 2020[iii], with retail ecommerce sales predicted to reach US$7 trillion in retail ecommerce sales by 2024[iv]. In 2021, organisations will continue transitioning to digital channels to reach customers, and need to confidently build new trust and loyalty models with their stakeholders.

Trust is hard won but easily lost today, and although ethics and values are increasingly prized by shareholders, investors and boards, we found that when it comes to customers, getting the basics right is most important. Okta's Digital Trust survey found that 32% of Australians, compared to 39% of global respondents, said service reliability was the criteria most likely to make them trust a digital brand—things like ensuring items arrive on time and in good condition. Security was also key for them: a quarter (24%) said that having secure log-in options such as multi-factor authentication (MFA) and other measures in place would help to nurture trust in a brand. This necessity for security was further felt by respondents in the UK (25%), the US (23%), Germany (22%) and the Netherlands (22%).

What is most important for consumers when it comes to trusting a digital brand?

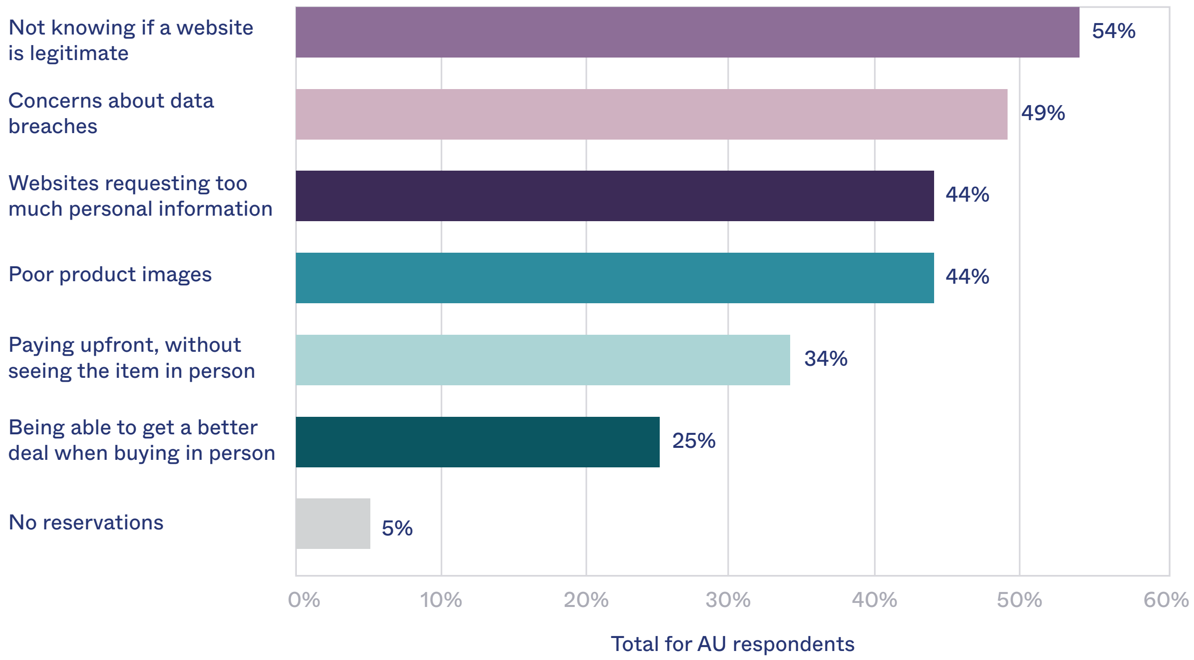


[iii] [iv] https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Brand reputation and online shopping

Brand awareness and reputation is closely linked to digital trust, and plays a big role in where Australians spend their money online. More than half (54%) of Australians indicated they would have reservations purchasing goods and services online if they hadn't previously heard of the brand. Coming in second, nearly half (49%) of Australians expressed concerns about data breaches. This is a clear message that Australians are taking brand reputation more seriously than ever, with awareness around the impact of data breaches on the rise. If private and confidential customer information has been compromised – whether intentionally or unintentionally released – this would have a detrimental impact on whether Australians would purchase from that brand again. Being asked to share too much personal information is also a cause for concern, with 44% of Australians saying this would impact their decision to purchase online goods or services from a brand.

What reservations do Australians have when purchasing items and/or services online?



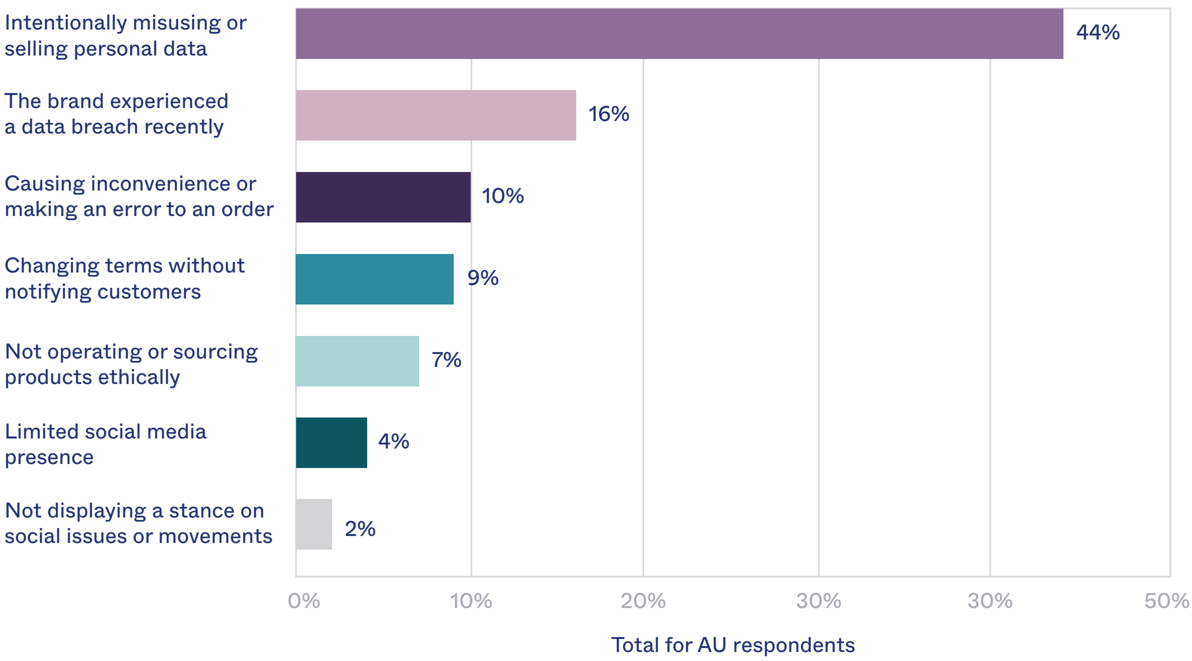
Breaches matter

So, what causes Australians to distrust a digital brand? The top two attributes cited by respondents were intentionally misusing or selling personal data (44%) and data breaches (16%).

Both are not only a matter of ethics for digital brands but practices that would draw the ire of the Australian Information Commissioner. To escape the wrath of customers and a potentially major reputational and financial fall-out, organisations must ensure their data security is fit-for-purpose—starting with best practice identity management.

The intentional misuse or selling of data was also the top attribute for distrusting a brand by all other markets. While data breaches were the second highest concern for respondents in Australia (16%), the US (15%) and the Netherlands (13%), inconvenience or errors were a more prominent factor in breaking trust for those in France (23%), Spain (21%) and Sweden (16%). This is a reminder that while data ethics remain of the utmost importance, seamless customer service is paramount.

What is most likely to cause Australians to distrust a digital brand?



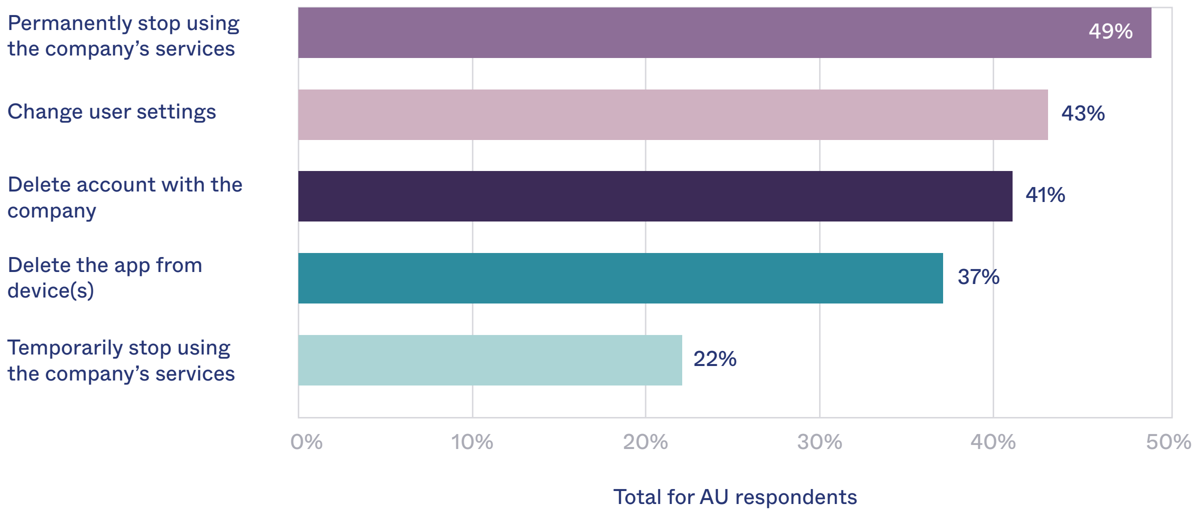
When trust is broken

It's clear that trust is vital for digital brands to succeed in today's highly competitive business landscape. 77% of Australian respondents said they would be unlikely to purchase from a company they didn't trust, and 54% admitted that they would have serious reservations about shopping on a website they'd never heard of before.

Once they've gained that trust, brands should be in no doubt that they must work hard to retain it, and that effective cybersecurity is key to them doing so. Two-fifths (40%) of Australian respondents said they'd lost faith in a company due to a data breach, with this figure much higher in the US (56%). Following a data breach, nearly half (49%) of Australian respondents said they would permanently stop using the company's services and 43% would change user settings such as passwords and email addresses, highlighting the importance of secure logins to maintaining ongoing trust. A further 41% would delete their account with the company.

49% of Australians would permanently stop using a company's services as a result of a data breach or misuse of data, while 41% say they would delete their account altogether.

What reaction would Australians take after losing trust in a brand due to a data breach or misuse of data?



There's work to be done to build trust

There’s still a great deal of work to do. Some Australian respondents (14%) said they don’t trust any digital channels to safely handle their data, similar to those in the UK (13%), the US (19%), Japan (22%) and Germany (23%).

By far, the most trustworthy of all digital channels in Australia is government websites (41%), with a similar sentiment felt by respondents in the UK (41%) and the Netherlands (37%). This is undoubtedly a positive. Despite initial concerns over handling of citizens’ COVID-19 and personal details during the pandemic, no breaches of this data have been reported in Australia to date, and continued scrutiny appears to be driving high standards of data security.

Websites and applications used for both work and play are trusted by fewer Australian respondents than government websites. Those used for work, including search engines and online databases, were rated the second most trustworthy at 17%, followed by enterprise communications apps, such as Zoom, Slack, Teams, Skype (10%), with established social media platforms, including Facebook, Twitter, Instagram, trailing behind (5%).

> Australians trust government websites to safely handle their data at a far higher rate (41%) than other channels.

How the pandemic has increased awareness of cyber threats

Over one third (35%) of Australian respondents said they “always” or “often” work from home today, and these same employees want more flexibility in WFH policies once the COVID-19 crisis has receded. Yet whilst isolated at home and away from their corporate networks, many have been exposed to an uptick in cyber-threats aimed at stealing both their corporate logins and personal identity data.

Phishing has been the preferred tactic of many cyber-criminals in 2020. They’ve had success using the lure of information on COVID-19 vaccines, or urgent (but fake) updates from trustworthy institutions like the WHO, to trick recipients into clicking through. In April 2020, Google alone said it was blocking 18 million daily malware and phishing emails related to COVID-19. Working from home has made respondents more wary of phishing emails (45%), data breaches (43%) and even AI-generated “deepfakes” used to spread false information (37%).

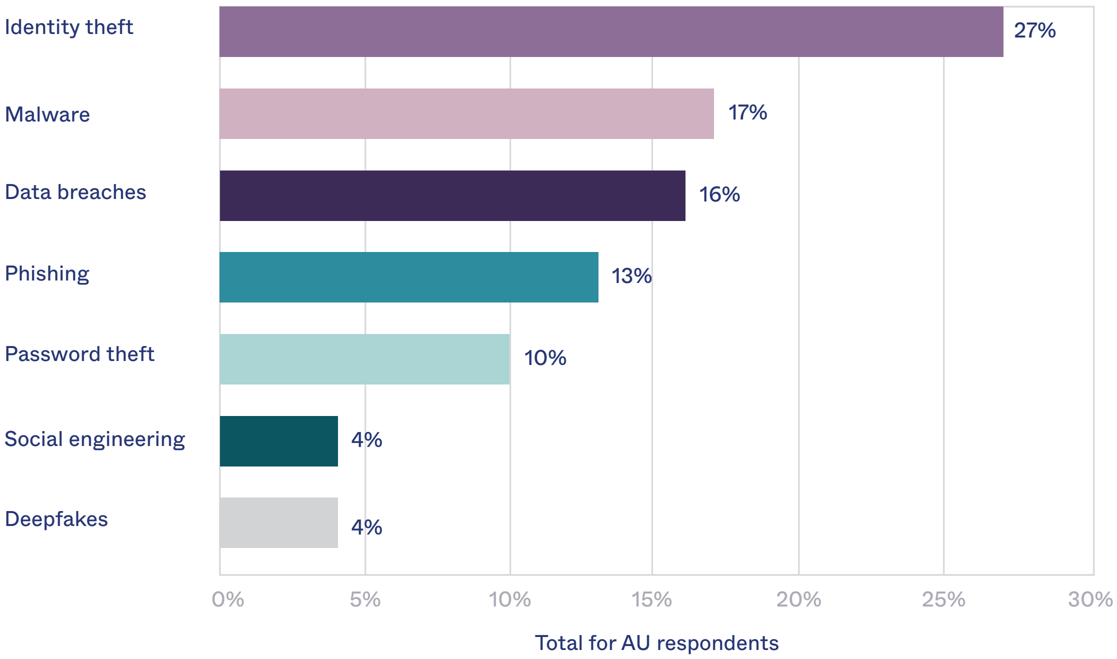
[v] https://cloud.google.com/blog/products/identity-security/protecting-against-cyber-threats-during-covid-19-and-beyond

Going forward, respondents feel they're most at risk from identity theft (27%), which is understandable given the increase in phishing attacks many have been subjected to. Malware (17%) and data breaches (16%) rounded out the top three concerns.

Interestingly, password theft posed somewhat of a low concern for respondents across Australia (10%), the UK (12%) and US (8%), which could indicate a complacency for misuse of personal or workplace digital accounts. It's worth remembering that an individual may be exposed to cyber-threats not only via attacks targeted at themselves and their devices, but by other users on their network who engage in risky behaviour online.

Australians feel most at risk of being exposed to identity theft (27%) and malware (17%) across personal/work devices in the future.

What security threats do Australians feel most at risk of being exposed to in the future?



Time to increase security education and transparency

Australians reported feeling more cautious overall (57%) about the safety of their data during the COVID-19 pandemic as opposed to those who felt no different (39%). Unsurprisingly, only 2% of Australian respondents reported feeling less cautious than before the pandemic.

The top reason given by Australian respondents for their increased caution online during the pandemic was media coverage about online threats (46%), which was the main reason for those in the UK (44%) and the US (37%). Consumers are clearly becoming more aware of the potential risks of engaging in the digital landscape, which means there's an opportunity for brands to improve awareness of how they are proactively tackling these challenges, thereby building trust. By taking a two-pronged approach of driving customer awareness and encouraging better account profile and credential management, such as offering multi-factor authentication (MFA) options, they can provide greater assurance to increasingly wary consumers.

There's a reason for employers to be more cautious as well. With more than a third of Australian respondents now regularly working from home or outside the office, there's a good chance employees are sharing devices and networks with family and friends. The low level of concern for the risk of password theft suggests employers need to raise awareness around online threats. Employers should consider educating staff on best practices for password hygiene, as well as updating any legacy tech that may be vulnerable to online threats. There is also an opportunity to demonstrate the effectiveness of security measures like endpoint anti-malware and anti-phishing solutions. This will help to build trust within organisations that provide the best tools for employees to manage working from home securely and productively.

Australians reported feeling more cautious about their data during the COVID-19 pandemic, largely due to media reports about online threats.

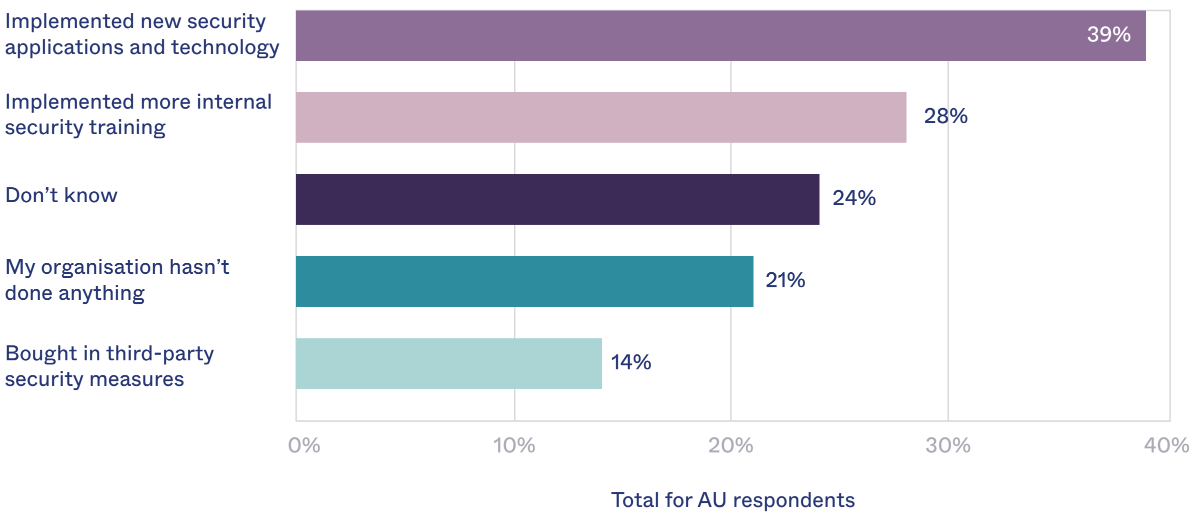
How are organisations responding?

Many employers have taken steps to tackle the growth in cyber-threats facing their home workers. New security applications and technologies like MFA (39%) are the most popular measure, followed by enhanced training for staff (28%). Both are vital in helping to drive the employee trust on which successful businesses are built.

What's concerning is the fact that 21% of respondents claimed their employer has done nothing so far to combat a pandemic-related surge in online threats. Furthermore, almost a quarter (24%) told us they didn't know if their employer had taken proactive security steps, with a similar sentiment felt by those in Sweden (40%), the UK (34%) the Netherlands (34%) and Japan (33%).

This potentially points to a lack of transparency between business and IT leaders and their employees. You could be running the best cybersecurity systems in the world, but if your staff doesn't know about it, your business will not be able to foster greater compliance and trust with its staff.

What measures do Australians report their organisations have taken to tackle the risk in cyber security issues?



Conclusion

As digital transformation opens new channels to engage with customers and support employees, and the cyber-attack surface expands in parallel, maintaining trust is imperative to the success of any business. Digital trust not only helps to mitigate harm, but also drives loyalty, revenue and value for organisations.

Today's digital-first businesses must constantly nurture trust as responsible stewards of customer data. Doing so will drive loyalty and success, even as cyber criminals continually step up their efforts.

For businesses, trust starts with establishing secure channels of communication and mitigating cybersecurity risks. To drive effective security measures, you must define the trust parameters by which employees, partners and customers access sensitive data and systems.

For stakeholders, trust also begins with security. The best way to become a more trusted institution among employees, customers and partners is by offering effective security tools and policies. Securing profiles (or digital identities) for all users communicating or transacting with a business is fundamental to enhancing productivity and building loyalty and engagement.

Survey Methodology

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 15,169 office workers from the US, the UK, Australia, Germany, France, Italy, Spain, Sweden, the Netherlands and Japan. This included 1,004 office workers from Australia. Fieldwork was undertaken between December 1 - December 27, 2020. The survey was carried out online.

About Okta

Okta is the leading independent provider of identity for the enterprise. The Okta Identity Cloud enables organisations to securely connect the right people to the right technologies at the right time. With over 6,500 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 9,400 organisations, including Engie, JetBlue, Nordstrom, Takeda Pharmaceutical, Teach for America, T-Mobile and Twilio, trust Okta to help protect the identities of their workforces and customers.