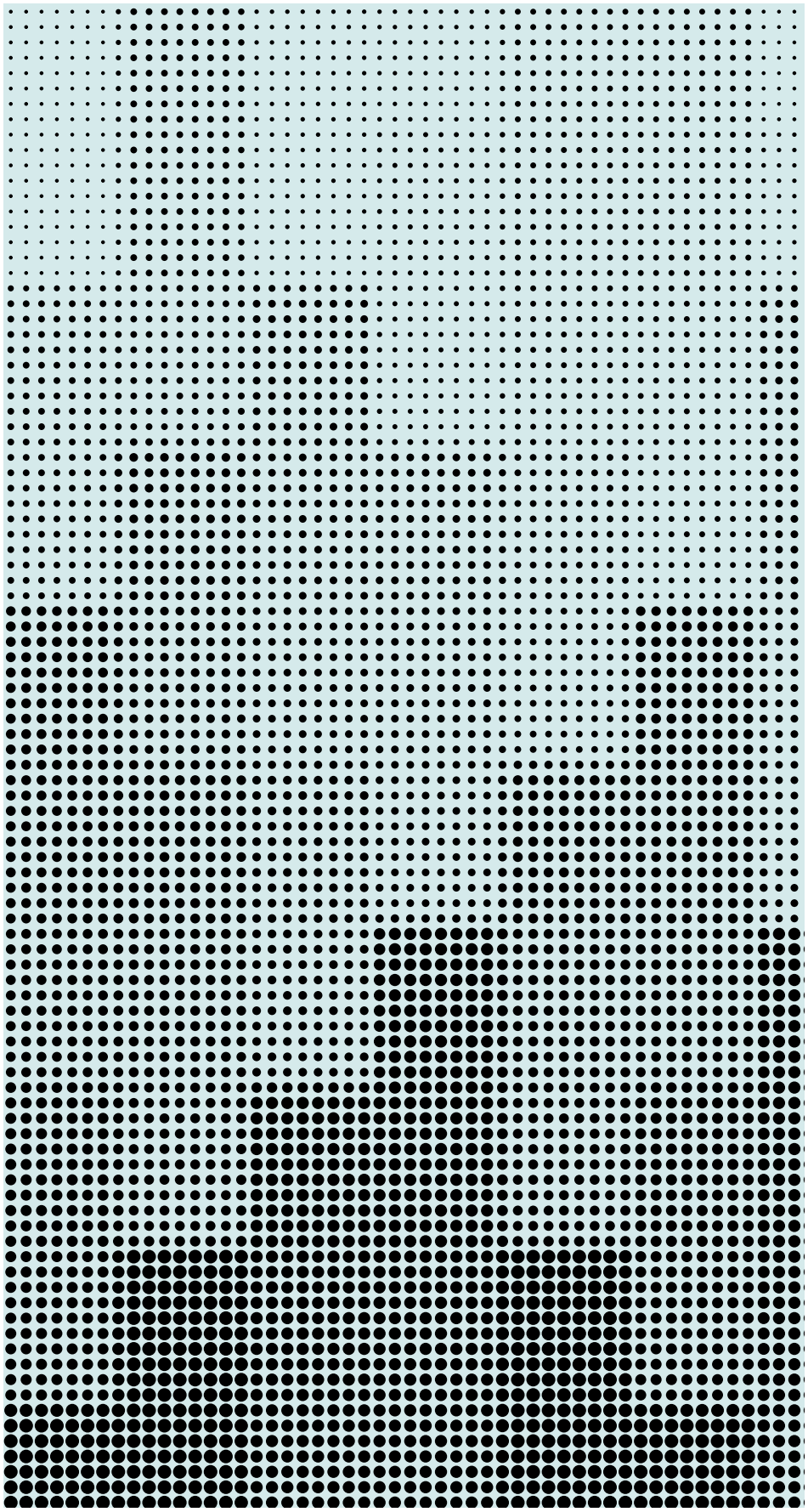
DATA REPORT

Hong Kong, Singapore, Philippines, Malaysia and Indonesia

May 2021

The State of Digital Trust

A snapshot of trust in an increasingly digital Asian 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 our governments 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 Singapore's Cyber Security Agency, which, as early as February 2020, warned that malicious emails purporting to inform users of how to protect themselves from the coronavirus, or provide an update on the situation, were being used by hackers to steal victims' information[i]. 2020 saw organisations around the world impacted by malicious cyber attacks, 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 1,700 office workers across Asia, in Singapore, Hong Kong, Philippines, Malaysia and Indonesia. This followed a global survey of more than 15,000 office workers in the US, UK, France, Germany, Italy, Netherlands, Spain, Sweden, Australia and Japan[ii]. 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 Asia, consumers care most about the core competencies: service reliability, strong security, quick response times 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.straitstimes.com/tech/wuhan-virus-hackers-exploiting-fear-of-bug-to-target-computers-gadgets

[ii] https://www.okta.com/the-state-of-digital-trust/

Key takeaways

Trust is fundamental to consumers: The events in 2020 led to trust becoming fundamental online, with 58% of Asian respondents saying they would be unlikely to purchase from a company they didn't trust. Getting the basics right is most important, with 26% 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 23% telling us that having secure log-in options and other measures in place would help to nurture trust.

Brand reputation impacts online shopping: Asians take brand reputation seriously when it comes to where they spend their money online. If they have concerns about data breaches (45%), believe images misrepresent products (39%), don't know if a website is legitimate (38%), or the website requests too much personal information (38%), many would have serious reservations about purchasing goods and services online.

Data ethics plays a key role: The top two reasons Asians would lose trust in a brand are 1) knowing they were intentionally misusing or selling personal data (34%) and 2) falling prey to a data breach (18%).

Websites used for work are most trusted: The most trustworthy of all digital channels are websites like search engines and online databases used for work, according to 25% of respondents from Philippines, Indonesia, Malaysia and Hong Kong. However, 47% of respondents from Singapore most trust government websites, while 10% of all Asian respondents 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. Half (50%) of Asian respondents said they have lost faith in a company due to a data breach or security event. Following an event, 44% said they had changed their user settings, such as passwords and email addresses. A further 38% said they had permanently stopped using the company's services and deleted the app from their device(s).

Office workers in Asia have become much more cautious online: With the rise of cyber threats over the past year, 71% of respondents say they have become more cautious about providing personal information about themselves online. Working from home practices have also made approximately 60% of respondents more wary of phishing emails, data breaches and even AI-generated "deepfakes" used to spread false information.

Media coverage is key in disseminating information about online threats: Asians have increased caution online during the pandemic for the most part due to media coverage about scams and cybersecurity threats (41%).

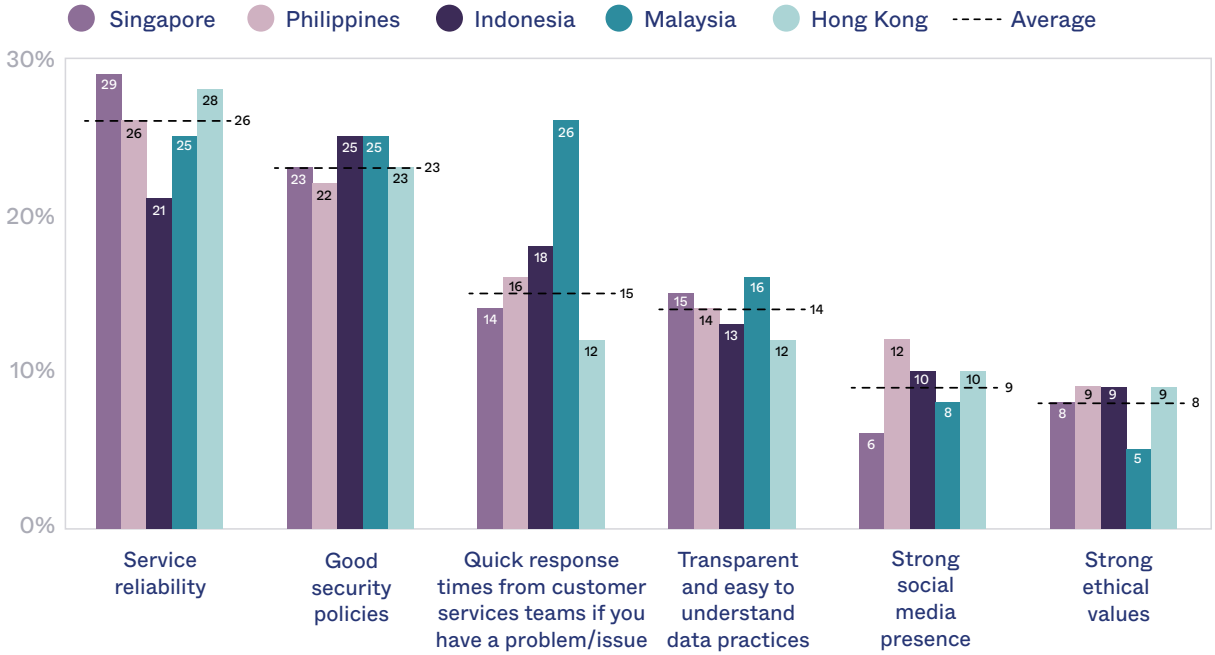
What makes consumers trust brands?

In 2020, as the world locked down and shifted to remote working, office workers spent a lot more time and money online. Asia-Pacific far outpaces other regions when it comes to retail e-commerce, with online sales growth nearly double that of the rest of the world[iii]. Looking at data from Singles' Day 2020 specifically, there were record spikes in online sales and traffic across Southeast Asia, with Malaysia seeing the highest increase in indexed sales at 600%[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 26% of Asian office workers, 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. Breaking down the findings by country, service reliability was most important to Singaporeans (29%) and least important to Indonesians (21%).

Security was also key for Asian respondents: 23% (increasing to 25% in Indonesia and Malaysia) 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 global respondents in the UK (25%), Australia (24%) and the US (23%).

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



[iii] https://www.bain.com/about/media-center/press-releases/2020/asia-pacific-retail-leads-world-with-three-quarters-of-global-growth-offering-a-glimpse-of-the-digital-future/

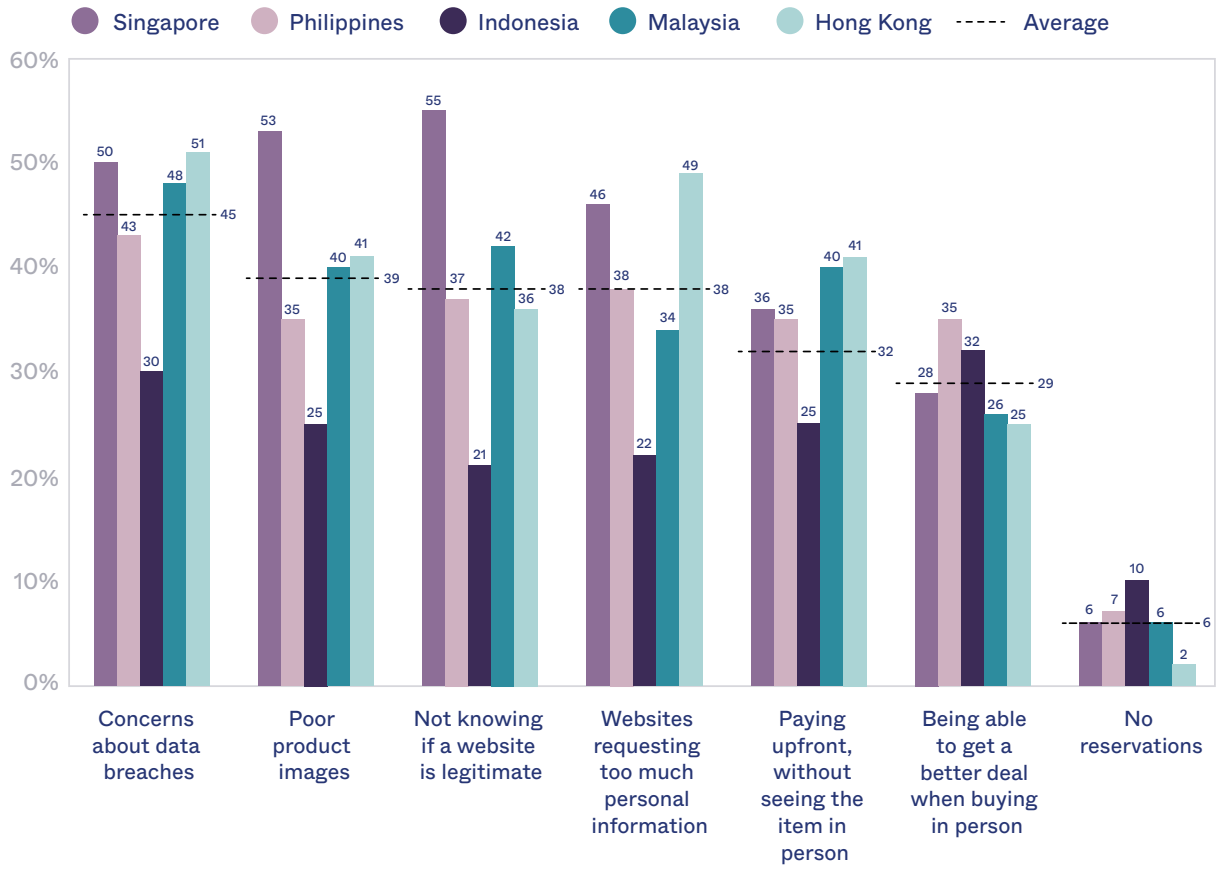
[iv] https://www.warc.com/newsandopinion/opinion/six-trends-apac-brands-should-leverage-in-2021/4011

Brand reputation and online shopping

Brand awareness and reputation is closely linked to digital trust and plays a big role in where Asians spend their money online. When asked about what would most deter them from purchasing goods and services online, 45% of Asian respondents (increasing to around 50% in Hong Kong and Singapore) listed data breaches as their top concern. This is a clear message that Asians are taking brand reputation and the security of the information they share online seriously, with awareness around the impact of data breaches on the rise.

Respondents were also unlikely to purchase from a website with poor product images (39%), that requests too much personal information (38%), or that looks illegitimate (38%). Singaporeans were the most discerning, with more than half claiming they would steer clear of websites that look illegitimate (55%) or display poor product images (53%).

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



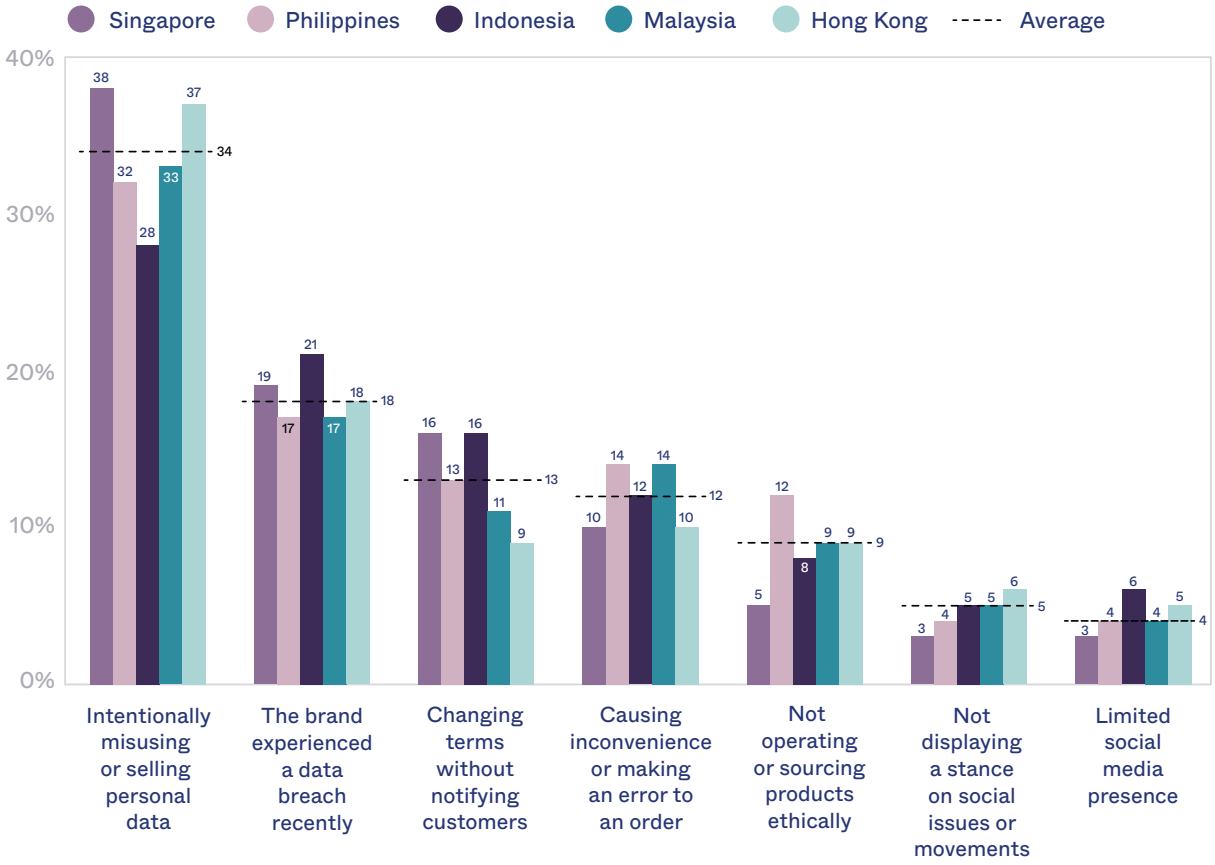
Breaches matter

So, what causes Asians to distrust a digital brand? The top two attributes cited by respondents were intentionally misusing or selling personal data (34%) and recent data breaches (18%).

Both are not only a matter of ethics for digital brands, but practices that would draw the ire of the Asia Pacific Privacy Authorities (APPA). 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 global markets and data breaches were the second highest concern for respondents in Australia (16%) and the US (15%). Respondents from Singapore (16%) and Indonesia (16%) called out changing terms without notifying customers as a key issue affecting trust. This is a reminder that while data ethics remain of the utmost importance, seamless customer service is also paramount.

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



When trust is broken

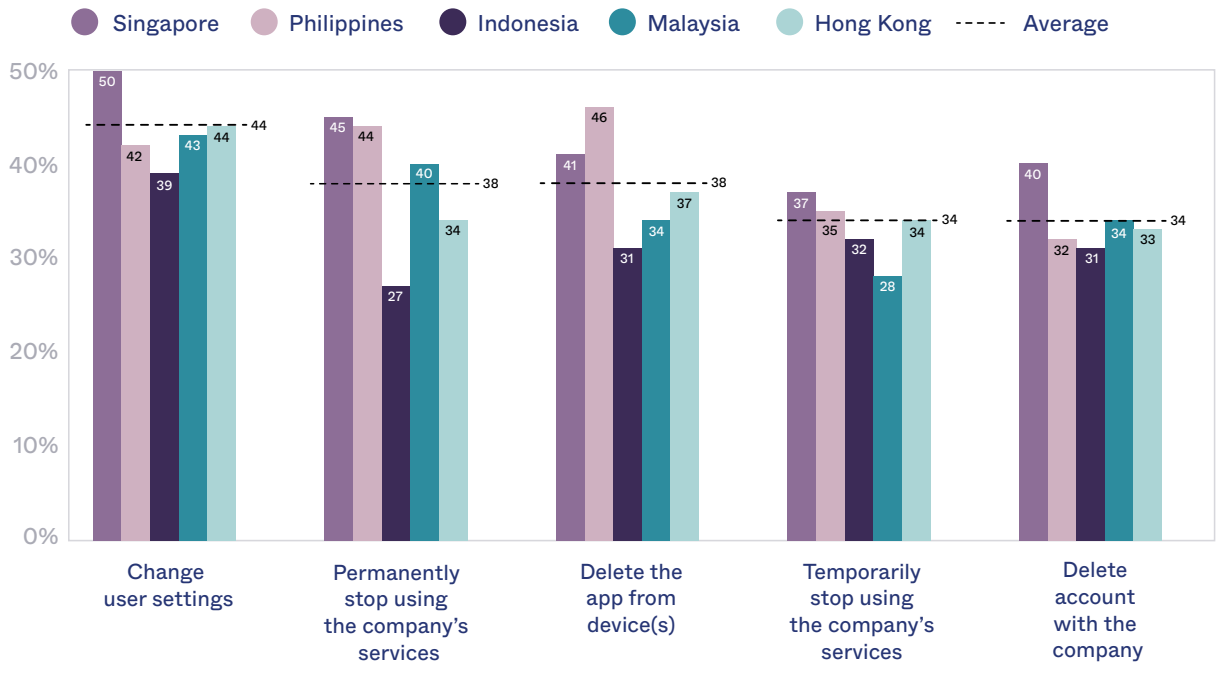
It's clear that trust is important for digital brands to succeed in today's highly competitive business landscape. 58% of Asian respondents (rising to 73% in Singapore) said they would be unlikely to purchase a product from a digital brand they did not trust. However, this is lower than respondents in other markets, where 77% of Australian, 75% of US and 88% of UK respondents say they would be unlikely to purchase from a company they didn't trust.

Once they've gained 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. Half of Asian respondents (50%) said they had lost faith in a company due to a data breach, compared to 40% in Australia and 56% in the US.

Following a data breach, 44% of Asian respondents said they had changed user settings such as passwords and email addresses, highlighting the importance of secure logins to maintaining ongoing trust. Furthermore, 38% said they had permanently stopped using the company's services and deleted the app from their device(s), and 34% deleted their account altogether. This lags behind Australia, where 49% said they had permanently stopped using the company's services and 41% deleted their account.

38% of Asians have permanently stopped using a company's services as a result of a data breach or misuse of data, while 34% say they have deleted their account altogether.

What reaction would Asians 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 10% of Asian respondents said they don't trust any digital channels to safely handle their data, which rises to 13% in the UK, 14% in Australia and 19% in the US.

As measures were rolled out across Asia to contain the spread of COVID-19 in 2020, experts warned of the risk of privacy breaches[v] given many governments lacked adequate oversight and legislation to protect data privacy. Indeed, there were reports that details from an Indonesian COVID-19 testing database were leaked online[vi].

Nevertheless, the most trustworthy of all digital channels in Singapore is government websites (47%) – a sentiment shared by Australia (41%) and the UK (41%), but not by Asian neighbours in the Philippines (13%), Hong Kong (16%) or Indonesia (16%). Websites used for work, including search engines and online databases, were rated highly by respondents in all Asian countries except Singapore, with 31% in Philippines, 26% in Indonesia, 22% in Malaysia and 20% in Hong Kong indicating they were most trustworthy.

Communication applications used for both work and play are trusted by fewer Asian respondents than government and work websites. Apps typically for personal use, such as WhatsApp and Facebook Messenger are trusted by 13% of respondents (rising to 20% in Indonesia), followed by established social media platforms, including Facebook, Twitter, Instagram (12%, rising to 18% in Hong Kong), and enterprise communications apps, such as Zoom, Slack, Teams, and Skype (10%).

Most Asian respondents trust websites used for work purposes, while 47% of Singaporean respondents say they most trust government websites to safely handle their data.

How the pandemic has increased awareness of cyber threats

The majority of Asian respondents (61%) said they "always", "often" or "sometimes" 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 over the course of 2020 and into 2021. They've had success using the lure of information on COVID-19 vaccines, or urgent (but fake) updates from trustworthy institutions like the World Health Organization, 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 Asian respondents more wary of phishing emails (59%), data breaches (59%) and even AI-generated "deepfakes" used to spread false information (58%).

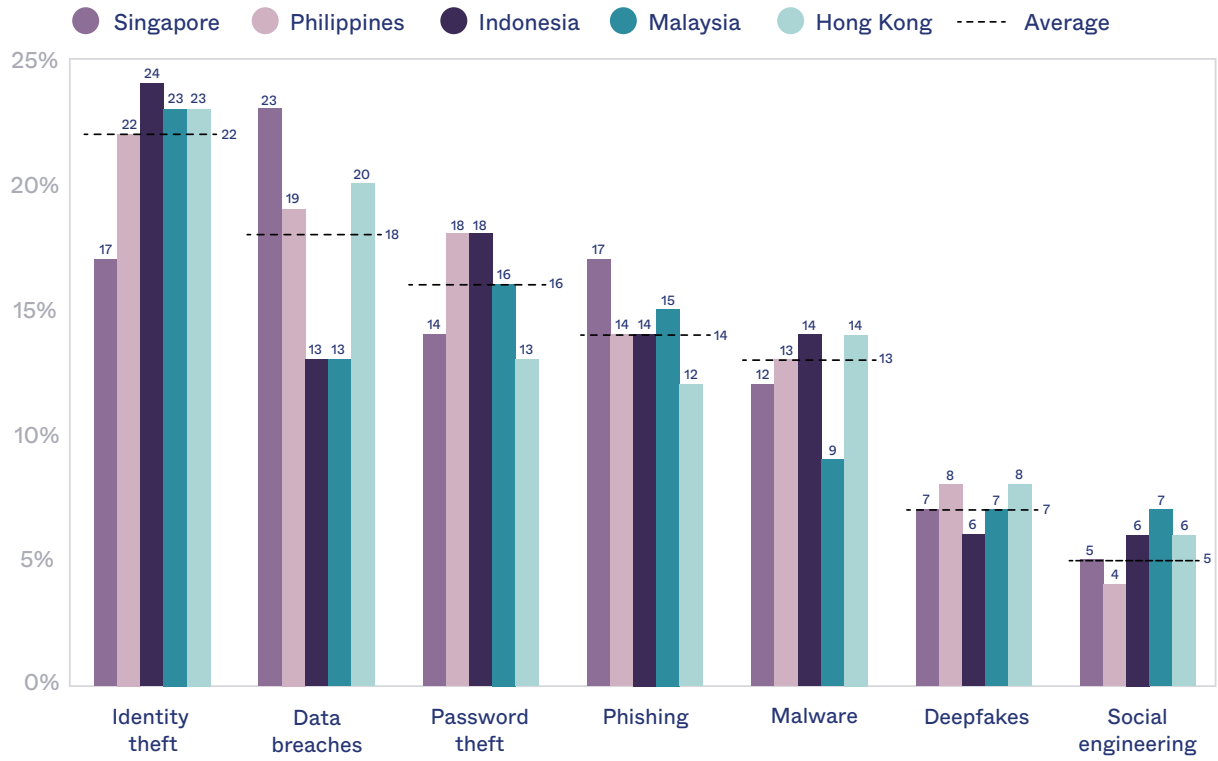
[v] https://www.reuters.com/article/us-health-coronavirus-privacy-idUSKBN26M40M
[vi] https://www.straitstimes.com/asia/se-asia/indonesia-probing-alleged-covid-19-test-data-breach

Going forward, respondents feel they're most at risk from identity theft (22%), which is understandable given the increase in phishing attacks many have been subjected to. Data breaches (18%) and password theft (16%) rounded out the top three concerns, with phishing following closely behind (14%).

Interestingly, data breaches posed somewhat of a low concern in Indonesia and Malaysia, with only 13% of respondents reporting they feel at risk of this threat. Deepfakes (7%) and social engineering (5%) rated relatively low across all Asian countries. It's worth remembering that an individual may be exposed to targeted cyber-threats without even realising they are in the crosshairs of an attacker.

Asians feel most at risk of being exposed to identity theft (22%) across personal and work devices in the future.

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



Time to increase security education and transparency

Asians reported feeling more cautious overall (71%) about the safety of their data during the COVID-19 pandemic, which was far higher than Australian respondents (57%) and global respondents (41%). 23% of Asian respondents said they felt no different and, unsurprisingly, only 3% of respondents reported feeling less cautious than before the pandemic.

The top reason given by Asian respondents for their increased caution online during the pandemic was media coverage about online threats (41%), which was also the main reason for those in Australia (46%), 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 nearly a third of Asian respondents (31%) 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 social engineering suggests employers need to raise awareness around online threats. Employers should consider educating staff on security best practices, 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.

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

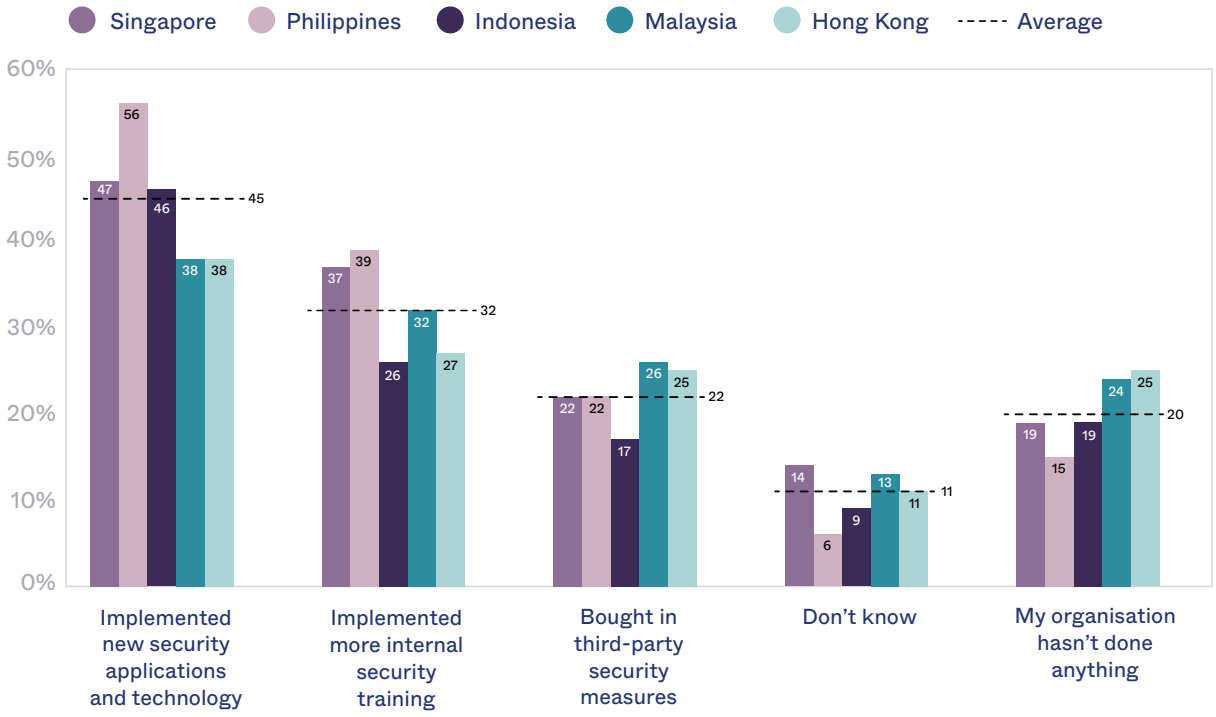
How are organisations responding?

Many employers have taken steps to tackle the growth in cyber-threats facing their home workers. New security applications and technologies like MFA are the most popular measure (45%, rising to 56% in Philippines), followed by enhanced training for staff (32%). Both are vital in helping to drive the employee trust on which successful businesses are built.

What's concerning is the fact that 20% of respondents claimed their employer has done nothing so far to combat a pandemic-related surge in online threats. Furthermore, 11% told us they didn't know if their employer had taken proactive security steps. While this is alarming, even more respondents were in the dark in Australia (24%), Japan (33%) and the UK (34%).

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 your business will not be able to foster greater compliance and trust if your staff doesn't know about it.

What measures do Asians 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.

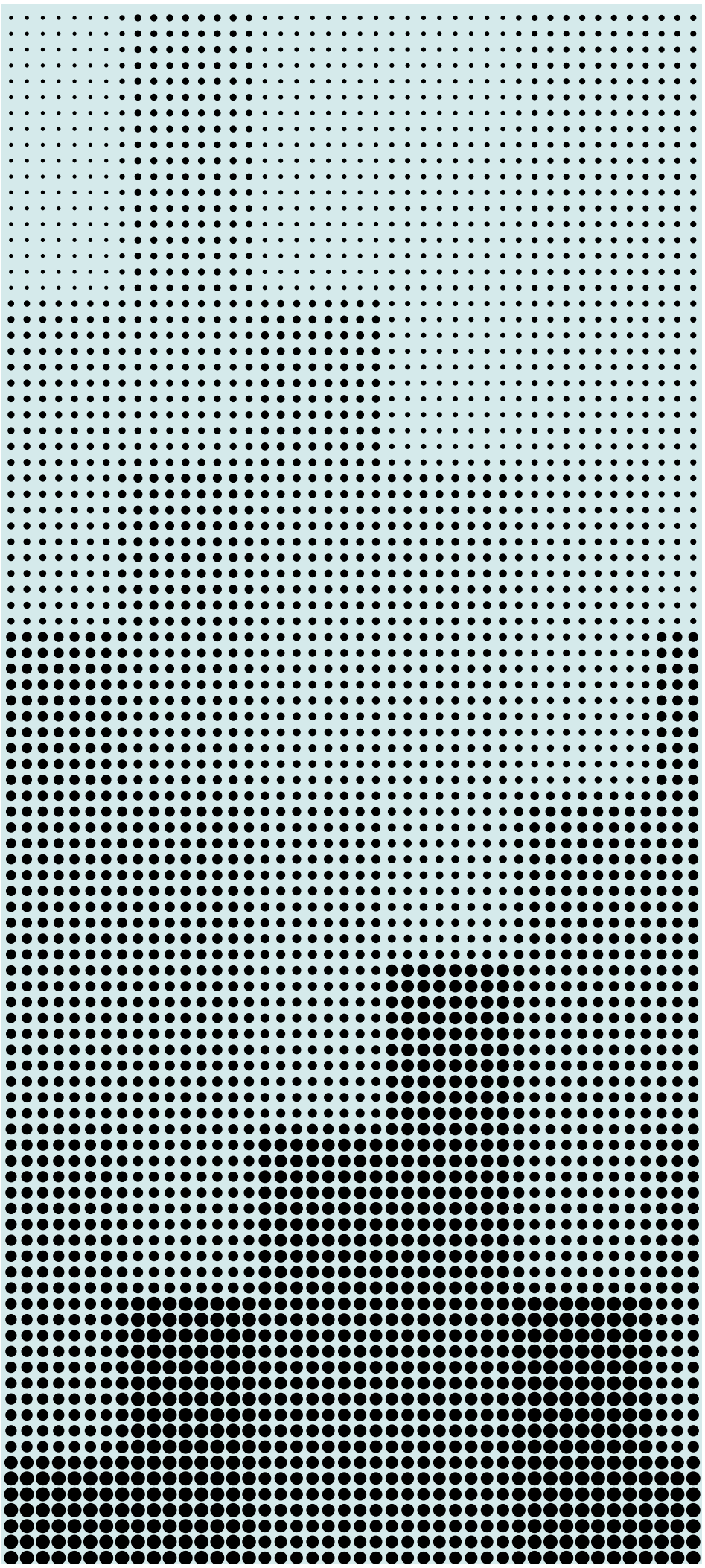
For stakeholders, trust also begins with security. The best way to become a more trusted institution among employees, customers and partners is by offering effective security tools and policies. Securing profiles (or digital identities) for all users communicating or transacting with a business is fundamental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

Survey Methodology

All figures, unless otherwise stated, are from YouGov Plc. Total sample size was 1,765 office workers across Asia, in Singapore, Hong Kong, Philippines, Malaysia and Indonesia. Fieldwork was undertaken between 12th – 24th March 2021. This followed a global survey of more than 15,000 office workers in the US, UK, France, Germany, Italy, Netherlands, Spain, Sweden, Australia and Japan, undertaken in December 2020. Both surveys were 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 7,000 pre-built integrations to applications and infrastructure providers, Okta customers can easily and securely use the best technologies for their business. Over 10,000 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.



okta