itnews
FOR AUSTRALIAN BUSINESS

The Digital Trust Challenge –

Securing customer identity management to ensure Digital Trust in an increasingly challenging era

Supported by

transmit security

Great customer experience is always important, but in today's on-demand digital world, customer identities and accounts are constantly targeted by evolving threats that demand advanced security and protection. However this presents a challenge for business leaders, that is, balancing great customer experience (CX) while ensuring security and privacy to which underpins customer trust. Digital trust is no longer a nice-to-have but a necessity. If organizations ignore their digital trust posture, customers will seek other service alternatives and therefore lose out to competitors

Customer identity and access management (CIAM) is the discipline of managing who can access your online services in a secure and uncomplicated way, from the moment they touch your digital asset throughout the customer journey including account recovery.

Most organisations today have some form of customer-facing digital services, but many still lack the CIAM capability to keep up with the persistent security threats they face to ensure digital trust.

To understand how organisations will secure access to their applications with CIAM, iTnews and Transmit Security asked IT leaders about the importance of proper access management and how this is evolving with more options for access control. This includes evaluating risk predictors during the authentication and transaction flow coupled with real time fraud behavioural monitoring throughout the user session.

To detect sophisticated fraud attacks organisations now need a combination of real time behavioural navigation, behavioural biometrics, device attributes and more. All of this supports good hygiene and best practices to ensure digital trust.

> Customer identity and access management (CIAM) is the discipline of managing who can access your online services in a secure and uncomplicated way,

When it comes to CIAM, Australian organisations have many opportunities to improve how they secure and manage their customers' digital experiences.

The research found a high 82 per cent of Australian organisations offer at least one type of customer account digital service, from mobile portals to e-commerce, indicating a high demand for CIAM.

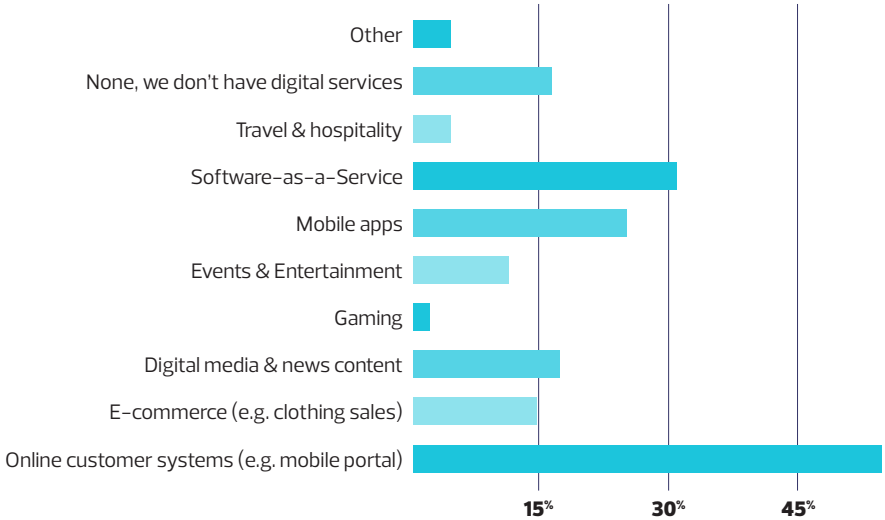
However, a similarly high 75 per cent have no dedicated CIAM capability, which presents a large security and process improvement gap.

DIGITAL CUSTOMER ACCOUNTS NOW A BUSINESS REALITY

Digital customer interactions have long been associated with the global "dot com" businesses such as Google and Microsoft, but the reality is most modern organisations now have some form of digital account management.

iTNews' research found a high 82 per cent of Australian organisations offer at least one type of customer account digital service.

Please indicate what type of customer account digital services your organisation offers

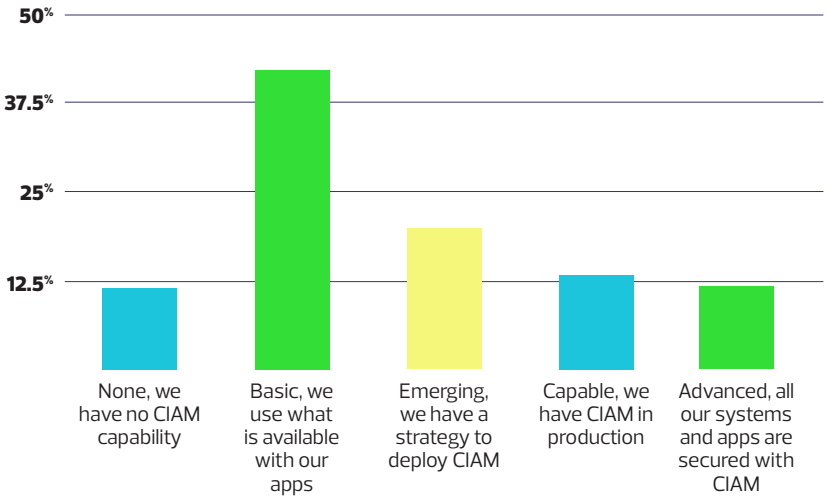


Moreover, the digital customer accounts are varied across a large number of use cases. From mobile portals to e-commerce, and from gaming to news content, Australian organisations are offering digital customer account services as part of their everyday operations.

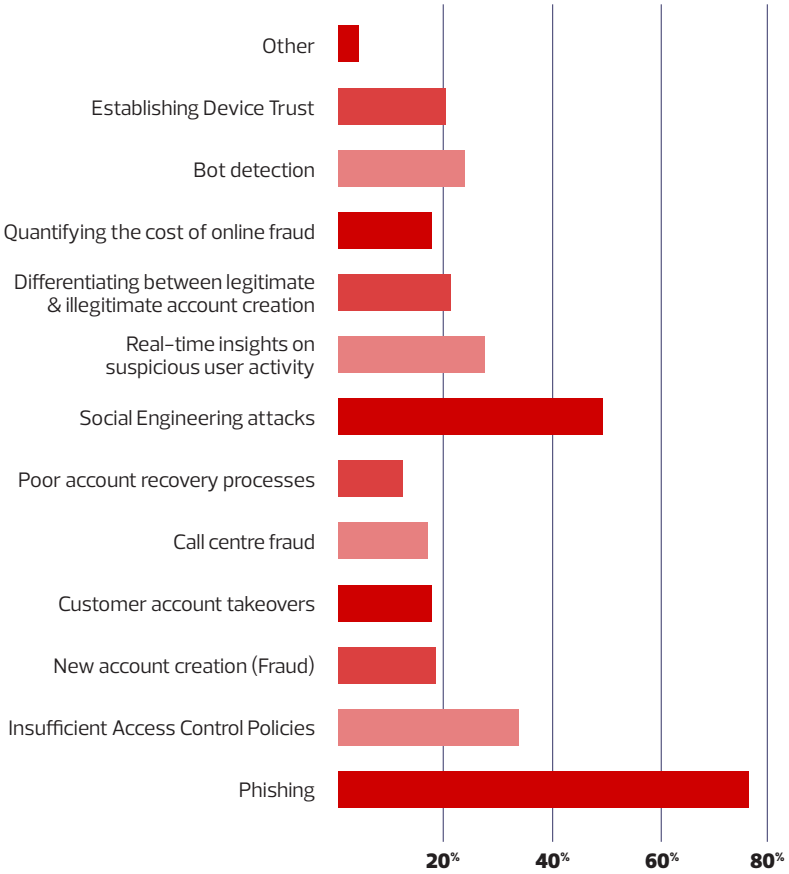
The discipline of customer identity and access management (CIAM) helps organisations secure and manage digital customer accounts and the research indicates a high demand for CIAM, even if IT leaders are not yet familiar with the benefits.

To discover more, the research asked what the typical maturity of an organisation is when it comes to CIAM.

What is your organisation's maturity when it comes to customer identity and access management (CIAM)?



What are your biggest challenges today around risk and fraud?



While slightly more than one in 10 have an advanced CIAM capability, 75 per cent have no dedicated CIAM capability at all, which presents a large security and process gap.

Furthermore, using only what is available with authentication and account management applications can give a false sense of capability, as such products are not specifically designed with customer security in mind.

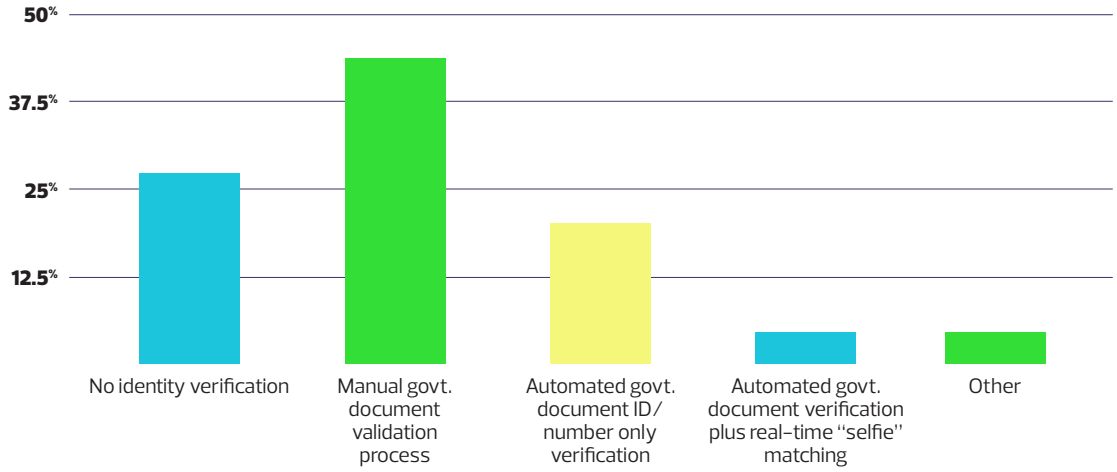
CUSTOMER ACCOUNT SECURITY REMAINS A CHALLENGE

Customers expect their accounts to be secure, and it is incumbent upon IT leaders to provide the best protection possible.

The research investigated what some of the biggest challenges Australian IT leaders face today around risk and fraud and many are associated with account management.

Phishing is a perennial challenge and 76 per cent of Australian organisations still see phishing as the biggest challenge around risk and fraud. Phishing can be an attack vector for unauthorised account access and controls should be in place to better verify how an account is accessed.

How do you currently complete Identity Verification for your customers?



Similar to phishing, other social engineering attacks were cited as a challenge for nearly half (49%) of IT leaders. Social engineering is a broad term for a variety of techniques which can be used to gain access to an account.

Fake messaging such as "sign in to receive a prize", or "you have been locked out of your account, sign in to regain access" can be used to harvest customer account details and should be mitigated with better controls.

In fact, the study found one in three respondents see insufficient access control policies as a challenge, and a further 27 per cent are not happy with the level of real-time insights on suspicious user activity they get.

The iTNews research is clear – many risk and fraud challenges relate to CIAM and there is a good opportunity for Australian organisations to improve their capability while increasing security.

IDENTITY VERIFICATION REMAINS LARGELY MANUAL

While IT leaders are well aware of the challenges with customer account management, the research uncovered significant shortfalls with how identity verification is performed.

A high 71 per cent of customer identity verification capability is still manual or missing entirely, and this includes 27 per cent of organisations which have no identity verification capability.

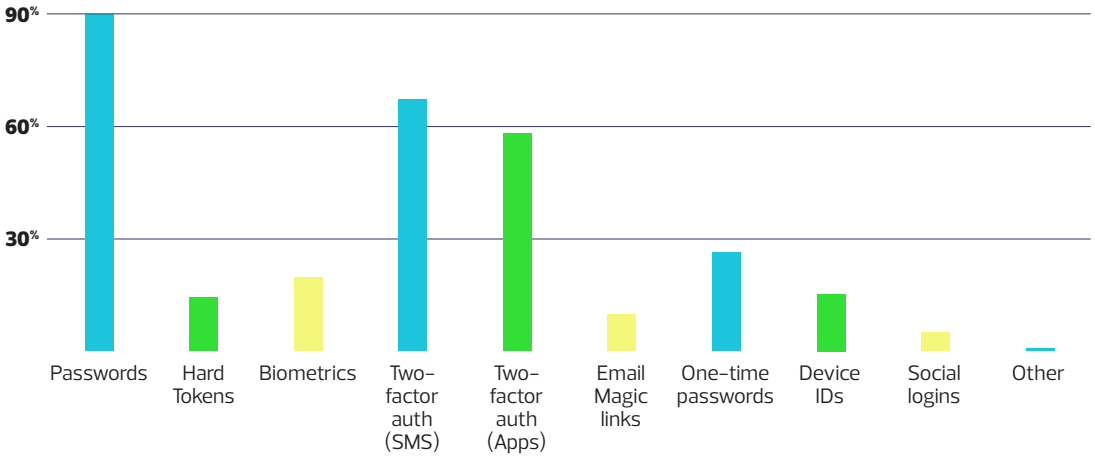
While IT leaders are well aware of the challenges with customer account management, the research uncovered significant shortfalls with how identity verification is performed.

A much smaller set have automated verification and only 4 per cent have automated document verification plus real-time "selfie" matching.

This capability gap has arisen due to a combination of the sheer volume of apps and cloud services used to manage customer interactions and a lack of easy to implement and manage CIAM solutions.

The research also investigated what customer access control measures are currently in use, and it was no surprise to see passwords on the top of the list with 90 per cent penetration.

What customer access control measures does your organisation currently use?



In an encouraging sign, two-factor authentication is the most popular access strengthening technique with 67 per cent of organisations using SMS and 58 per cent using apps.

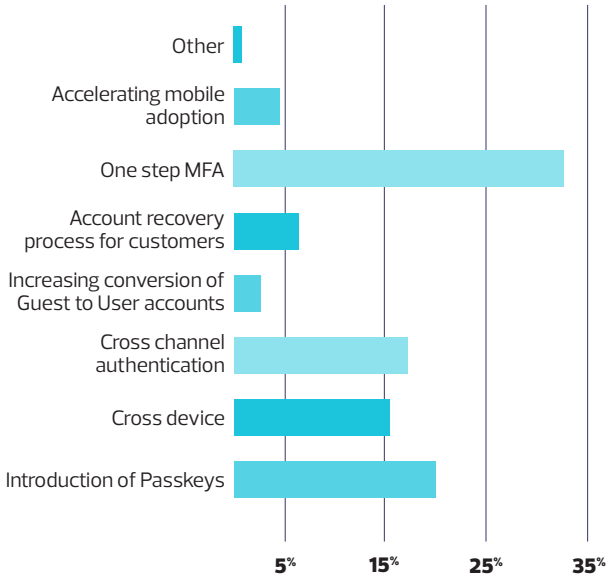
Lower down the list are one-time passwords and biometrics. While these tactics have been available for many years, they are still not widely adopted.

When asked which areas around authentication are of most relevance, or interest, to their organisation, about one-third of IT managers see one-step MFA as ideal for strengthening access beyond passwords.

Another tactic of interest is passkeys,. Passkeys are an extended version of FIDO (Fast Identity Online) credentials. They streamline and package the benefits of FIDO for multi-device use within a single ecosystem (for example within Apple, Google or Microsoft). However, you can't use passkeys between different ecosystems, nor can they extend trust to non-passkey devices or operating systems. IInstead of passwords, FIDO credentials are invoked with on-device authentication, like face recognition (e.g., FaceID) and fingerprint scanning (e.g., TouchID). Passkeys exist because passwords are on their way out. You don't need to be a security expert to know that passwords have a laundry list of problems. It is no surprise that one in five IT leaders are interested in passkeys and a further 17 per cent are interested in offering authentication across a number of channels whilst users adopt this new technology.

And when it comes to social logins, as a customer access control measure only around 5 per cent of organisations have implemented them.

Which of the following areas around Authentication are of most relevance or interest to your organisation



When asked which areas around authentication are of most relevance about one-third of IT managers see one-step MFA as ideal for strengthening access beyond passwords.

While Social logins are the most globally accessible type of identity, it can seem counter intuitive that their penetration with Australian organisations is low. As such, in order to understand the trend, we polled organisations about the views on social logins.

At this time most (59%) IT leaders have no need for social logins; however, around one in five would like to use social logins, but are not happy with the risk they bring.

About 15 per cent of the respondents reported using social logins for "low risk" applications, further indicating that uptake is minimal.

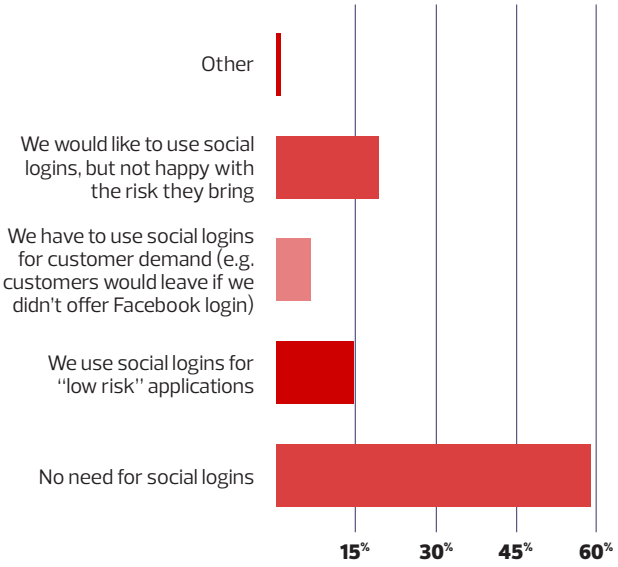
AWARENESS IN BETTER CIAM SOLUTIONS GROWING

As iTNews' research shows Australian organisations have a need for better customer account security, but still lack customer identity verification capability, which is manual or missing entirely.

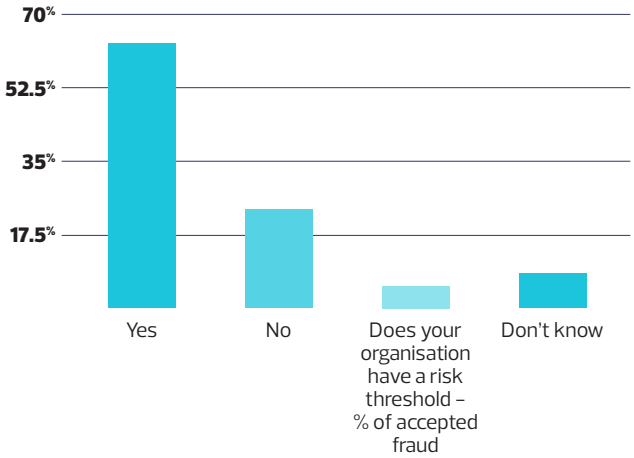
Customer identity and access management (CIAM) helps IT leaders manage who can access online services in a secure and easy way – from the moment they touch your digital asset throughout the customer journey including account recovery.

CIAM is not yet widely deployed, but awareness is growing with a high 63 per cent of IT leaders now more aware of the need for CIAM thanks to recent, high-profile data breaches.

What is your organisation's view of social logins? Social logins allow customers to use the credentials from a social network (e.g. Facebook, Google) to access your digital services.



Have recent high-profile data breaches made your organisation more aware of the need for CIAM?

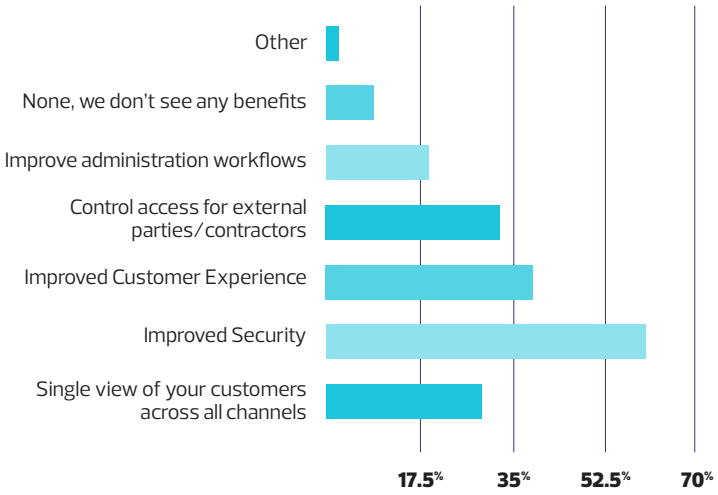


This increased awareness is in line with how IT managers view the benefits of CIAM, with more than 90 per cent believing CIAM does support business objectives, including improved security and customer experience.

More than one in three also believe CIAM can help control access for external parties, including contractors. With remote and hybrid working here to stay, third-party access management is now a fundamental part of security operations.

To reap the benefits, IT leaders must have a clear path to CIAM, and the research investigated what they see as the main challenges with CIAM.

Please indicate how CIAM currently supports your business objectives?



In your view, what are the main challenges with CIAM?

The number one challenge is a perceived difficulty for staff to configure and operate, followed by cost.

This indicates Australian organisations are ready for an easy, supported path to CIAM and this sentiment was clear in the research which found two in three IT leaders prefer a cloud or MSP delivery model for CIAM solutions.

With an on-demand CIAM solution, Australian organisations can strengthen their digital trust posture. Today, the digital world is where businesses compete, as such by leveraging CIAM to enhance customer onboarding, access, and security; organizations will be best aligned to compete and capitalize on the digital economy. ■

About the survey

This survey was conducted in November 2022 by iTnews on behalf of Transmit Security and attracted 110 respondents: 26.36% were IT managers or IT directors, 14.55% were IT professionals, including developers, analysts and engineers, and the rest included people in sales and marketing roles, CEOs, CFOs, GMs or MDs, those in analysis, consulting or education roles or similar, in addition to people in other roles. Looking at the size of their organisations, 26.36% worked for employers that have more than 2,500 staff members, 19.09% were at organisations with less than 10 people, while 17.27% worked for companies that employ 10–49 people.

transmit security

itnews FOR AUSTRALIAN BUSINESS