Securing Customer Identity Management in an Increasingly Challenging Era 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. Ensuring that great experience is secure is no longer a nice-to-have, but a necessity. Customer identity and access management (CIAM) is the discipline of managing

who can access your online services in a secure and easy way from the moment they touch your digital, or in-store, assets throughout the customer journey including account recovery.

Most organisations today have some form of customer-facing digital services, but many still lack the CIAM capabilities to keep up with the deceptive, automated security threats customers face. A solution that's purpose-built for customers should be able to protect accounts without hurting the customer experience. This requires accuracy that only an intelligent, context-aware solution can provide.

New insights into the emergence of CIAM 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 analysis of behavioural navigation, behavioural biometrics, device attributes and more. You must be able to correlate hundreds of signals to detect signs of account takeover fraud anywhere in the customer journey — from registration to account recovery and every step in between. 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.

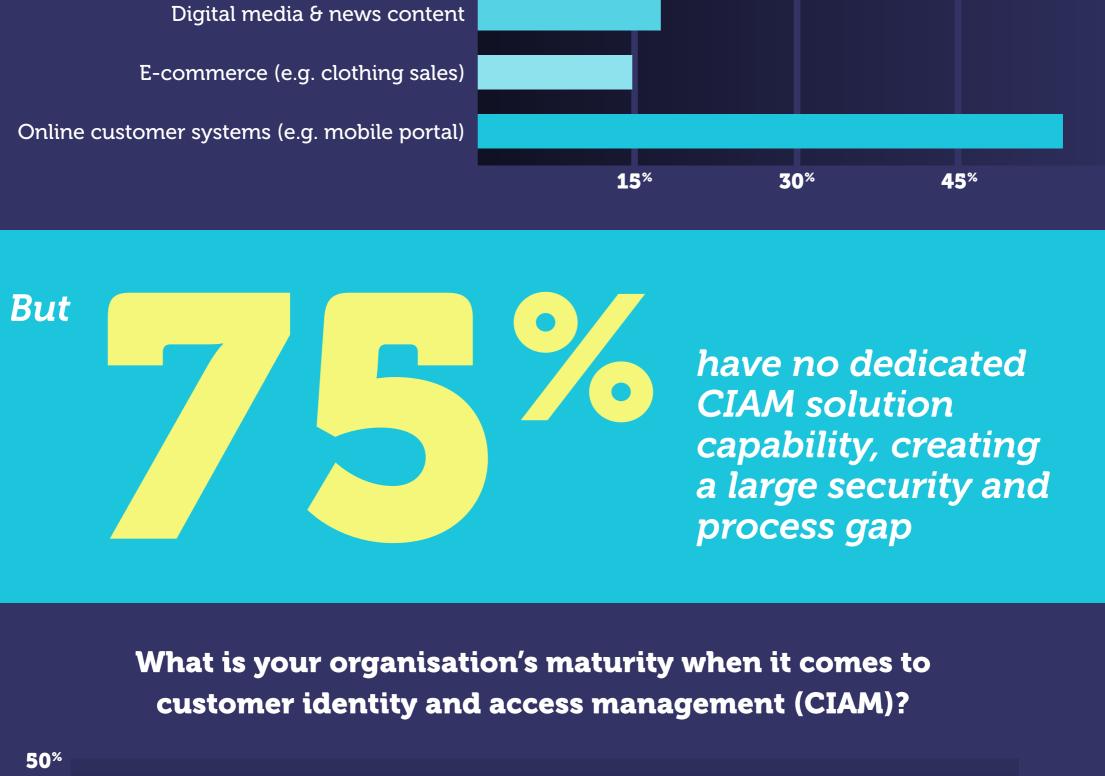
When it comes to CIAM, Australian organisations have many opportunities to

improve how they secure and manage their customers' digital experiences and accounts.

customer account digital

Other None, we don't have digital services Travel & hospitality

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



Capable, we Advanced, all None, we have no Basic, we Emerging, **CIAM** capability use what is we have a have CIAM in available with strategy to production deploy CIAM with CIAM our apps of Australian organisations still see phishing as the biggest challenge around risk and fraud

What are your biggest challenges today around risk and fraud?

Other

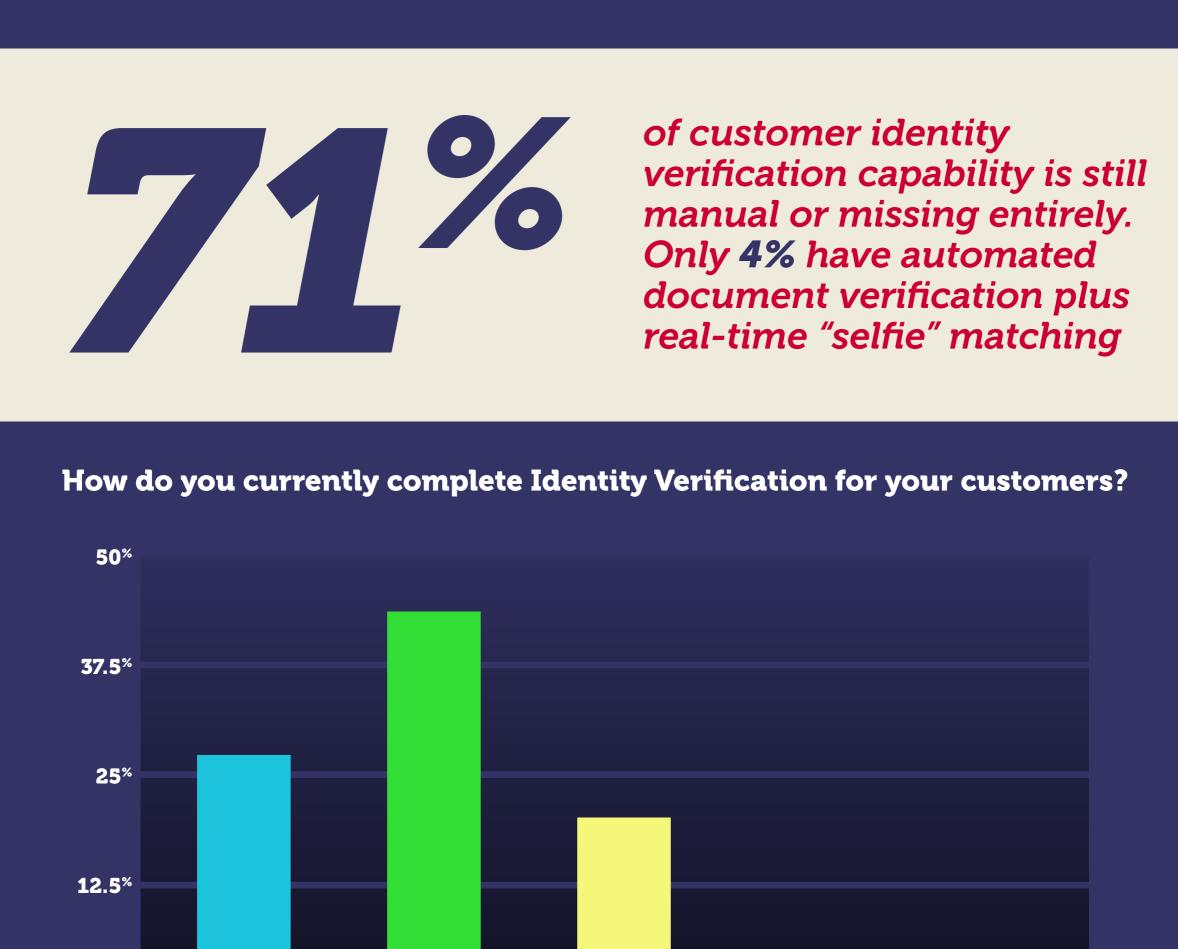
Bot detection

Establishing Device Trust

New account creation (Fraud)

Insufficient Access Control Policies

Quantifying the cost of online fraud Differentiating between legitimate & illegitimate account creation Real-time insights on suspicious user activity Social Engineering attacks Poor account recovery processes Call centre fraud Customer account takeovers



60%

Other

Other

Automated

govt. document

verification plus

real-time "selfie"

matching

80%

common customer penetration access control measure at What customer access control measures

does your organisation currently use?

Automated

govt. document

ID/number only

verification

Manual govt.

document

validation

process



standards for passwordless MFA with a fingerprint or facial biometric plus a private key stored on the device (no database of password data to steal). have no need for social logins and 19% would like to use social logins, but are not happy with the risk they bring 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. Other We would like to use social logins, but not happy with the risk they bring We have to use social logins for customer

Too expensive Too many products and solutions already deployed Lack of available products or solutions 10% 20% **30**% 40% However,

see benefits in how CIAM aligns with their supports

business objectives, including improved security

and customer experience

Please indicate how CIAM currently supports your business objectives?

Improved Security Single view of your customers across all channels **17.5**% **35**% **70**% **52.5**[%]

Other

None, we don't see any benefits

Improved Customer Experience

Improve administration workflows

Control access for external parties/contractors

of IT leaders more aware of the need for CIAM Have recent high-profile data breaches made your organisation more aware of the need for CIAM? **70**% **52.5**% 35% **17.5**%

have a risk threshold - % of accepted fraud

Мо

Yes

that employ 10-49 people.

IT leaders prefer a cloud service or MSP

Does your organisation Don't know

delivery model for CIAM solutions

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

of Australian organisations offer at least one type of online service, from mobile portals to e-commerce, indicating a high demand for CIAM

Software-as-a-Service Mobile apps Events & Entertainment Gaming

37.5% **25**% 12.5% our systems and apps are secured

Phishing 20% 40%

60% **30**% **Passwords** Biometrics Two-factor Two-factor Hard

No identity

verification

With passwords

being the most

90%

One step MFA Account recovery process for customers Increasing conversion of Guest to User accounts Cross channel authentication

5%

Lins

are interested in passkeys, an extension of FIDO authentication

15%

25%

35%

Cross device

Introduction of Passkeys

And

demand (e.g. customers would leave if we didn't offer Facebook login) We use social logins for "low risk" applications No need for social logins **15**% **30**% 45% **60**% challenge IT managers see with CIAM is that it's difficult for staff to configure and operate, followed by expense In your view, what are the main challenges with CIAM?

Other

Not a budgeted project

Difficult to deploy

Don't have executive buy in

Difficult for customers/users to use

Difficult for staff to configure and operate

And recent high-profile data breaches have made 63%

Zin