AN IDC INFOGRAPHIC

THE VALUE OF IDENTITY IN THE DIGITAL ENVIRONMENT

This IDC Infographic looks at identity management in reframing cybersecurity as an opportunity for Asia/Pacific businesses to gain a distinct advantage, especially amid uncertain times.

In the Face of the New Normal

CEOs' new mandate in the digital economy:

Trust

Engendering trust, defining new value, and ensuring reliable digital services and experiences rank highest in importance to the overall business vision.

Respondents were asked to rank their strategic business priorities, with 1 being the least important and 5 being the most important

Remote working as part of the Future of Work

Remote working is no longer a nice-to-have but a critical element of business resiliency and continuity plans, and for many, may become business as usual.

60% of Asia/Pacific employees surveyed want remote access, but only 40% have it

40% of Asia/Pacific respondents in banking and financial services cited productivity gains due to remote access.

Key Security Challenges

Security resource issues

30% of Asia/Pacific organisations suffer from a lack of skills to ensure reliable and secure digital services. The talent shortage is more critical in Singapore, while Australia and New Zealand are in line with the regional average.

Asia/Pacific average	Singapore	Australia	New Zealand
30%	55.6%	33.2%	33%

Insufficient security management focus

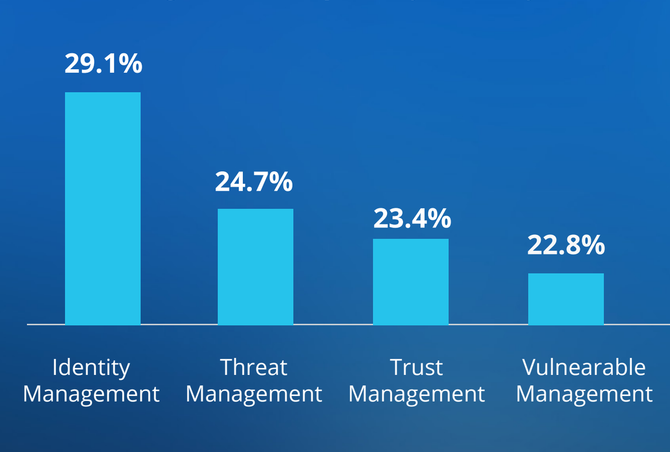
<10% of organisations have a dedicated chief information security officer (CSO or CISO).

80% For 80% of organisations, the head of IT (CIO or IT director) is also the head of security.

IAM headcount

Enterprises with at least 500+ employees surveyed by IDC have an average of 23 full-time employees in the IT security department, with more resources focused on IAM than any other area of IT security.

Considering the importance of threat identification, the ability to transfer valuable resources by improving IAM efficiencies would be considered a strategic move.



Looming identity crisis

Businesses are still warming up to MFA and federation for enhanced security.

23.4% of Asia/Pacific organisations plan to deploy MFA for all users accessing sensitive data.

30.4% of Asia/Pacific organisations are considering or piloting identity federation plans.

29.1% Disconcertingly, 29.1% surveyed are not even considering federation.

Remote working is here to stay

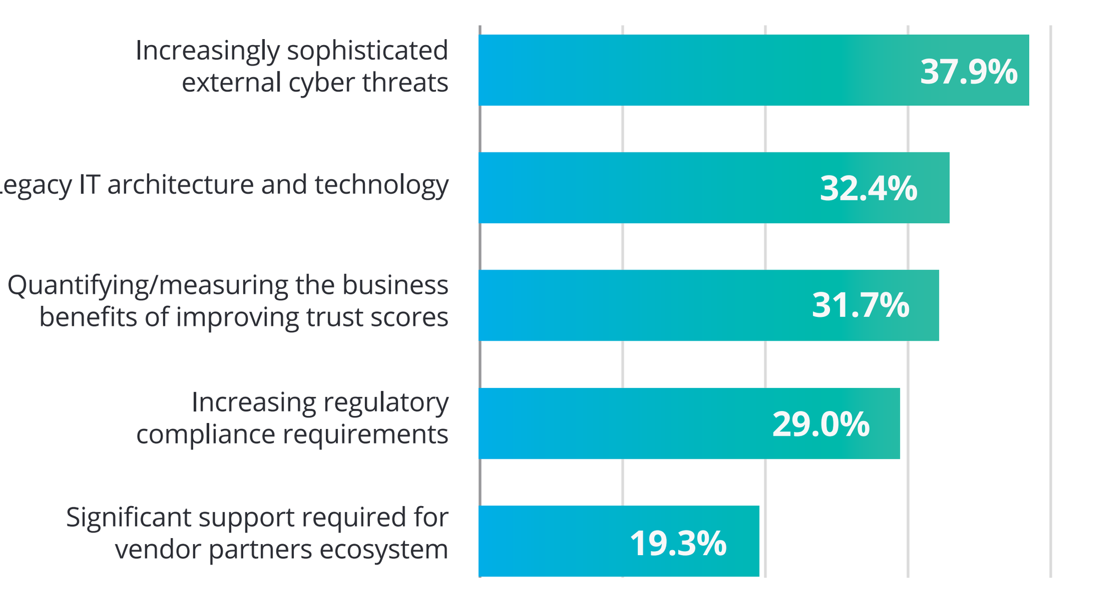
Business and IT leaders must address the security changes head on:

- Control over corporate network access from employees' managed and unmanaged devices.
- Addressing the complexities of authentication and compliance.
- Adopting a strong cyber risk governance practice.

Building a Trust Agenda Through Trusted Identities

Today's boardroom agenda **calls for a prioritisation on driving security,** specifically **identity.**

Strategic investment in IAM is one way to address many of these issues, particularly where users and identities are validated and monitored.



Data security and data privacy rely on user semantics, which means authentication of users is critical.

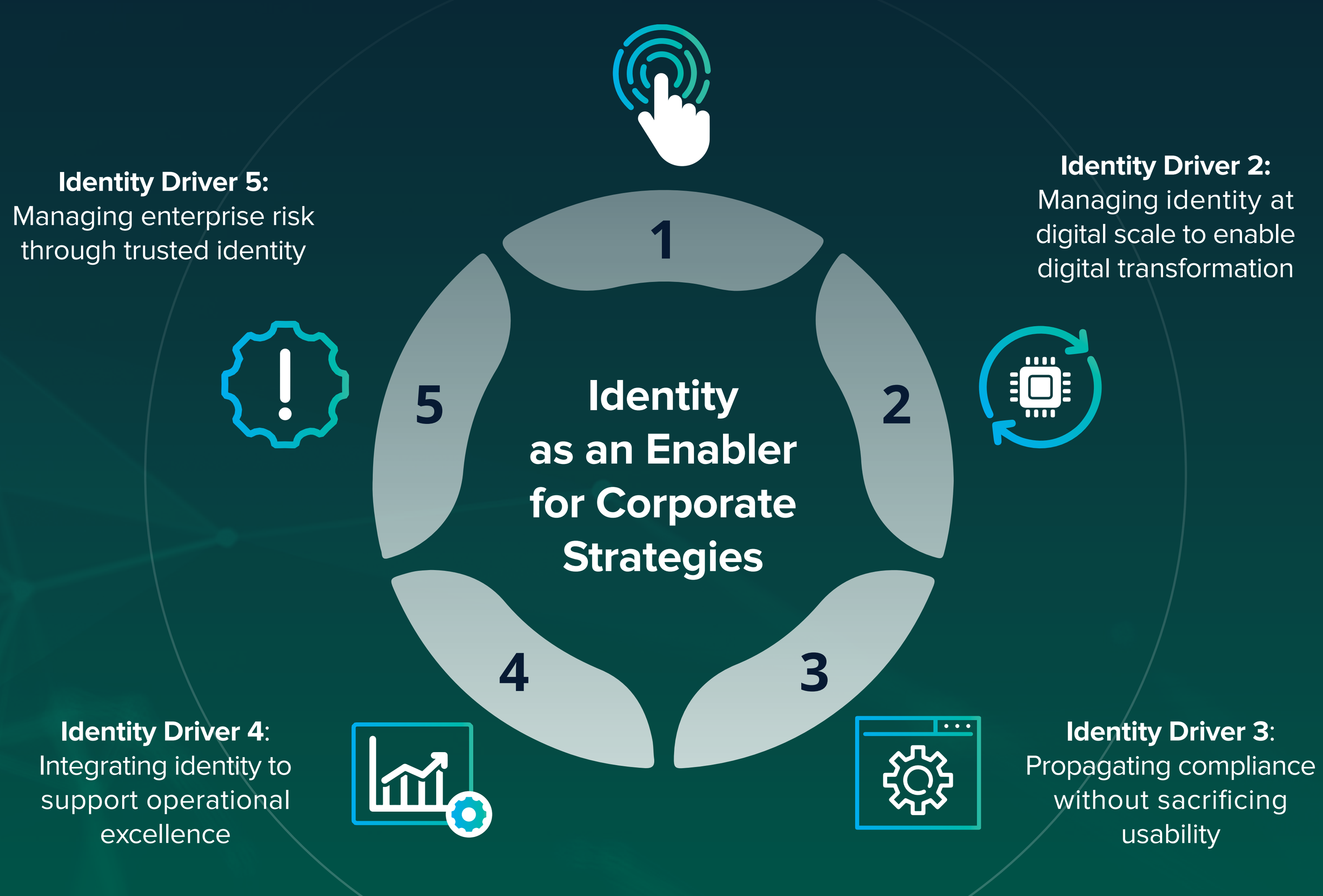
Passwords are still the ubiquitous method of accessing secure systems and so, naturally, become a critical asset, and a target for threat actors.

With security control points shifting to data, application and **identity**, the need for stronger identity management and security tools is paramount.

Identity is a unifier across the new security control points of identity, data, and application, so addressing IAM issues early can help to quickly resolve other areas of concern.

Source: IDC's CXO View of the Future Enterprise in the Digital Economy 2020

Identity as an Enabler for Corporate Strategies



Building a Trust Agenda With The Board

Security as the foundation

- Identity, along with applications and data, are emerging as the new control points.
- Ensuring data privacy is about who has access to what data, and in today's environment, from where.
- Data security is a key control point as it relates to both compliance and trustworthiness.

Changing models of IAM solutions

- Move away from single solution deployments.
- Look for a more consolidated suite of services that integrate seamlessly with other vendors.
- Multi-factor authentication, password management, and single sign-on, used in combination, offer a much-needed level of control and visibility.

The right tools

- Solutions with improved ease of use and greater automation help reduce time spent on user access requests and identity management to ensure better use of security resources elsewhere.
- Refocus staff to other critical security roles such as threat identification and remediation.
- IDC forecasts that cloud-based IAM will grow nearly 3 times as fast as on-premises IAM by 2023.

Are you ready to elevate the security conversation to a business one?

DOWNLOAD the IDC InfoBrief to learn more

Source: IDC InfoBrief, Sponsored by LogMeIn, The Value of Identity in The Digital Environment, May 2020

IDC ANALYZE THE FUTURE

Sponsored by: LastPass by LogMeIn