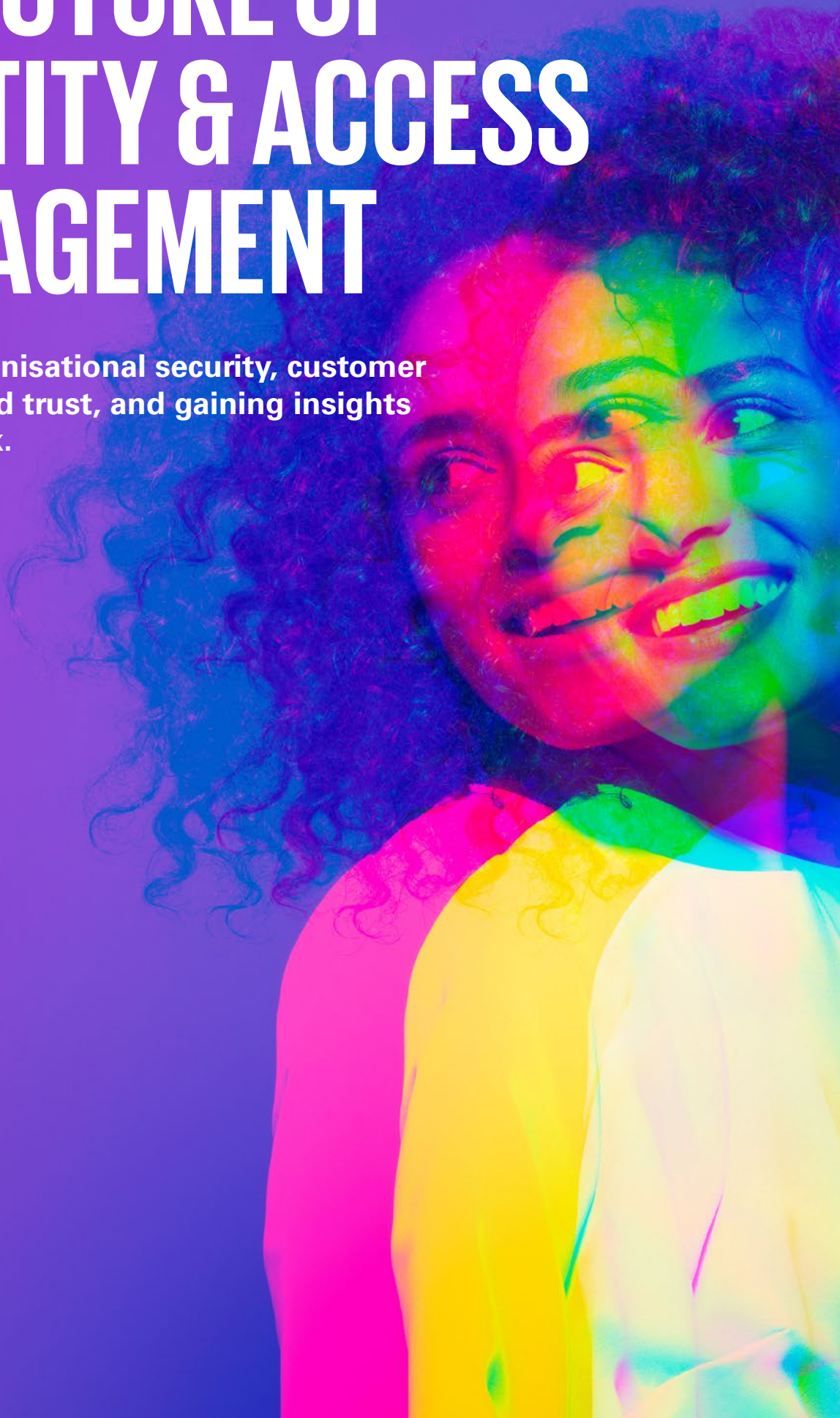
THE FUTURE OF IDENTITY & ACCESS MANAGEMENT

Improving organisational security, customer experiences and trust, and gaining insights for reduced risk.



KPMG

Contents

Introduction

Organisations and their workforces have endured rapid and profound change in the wake of the global COVID-19 pandemic, with 'hybrid' models that combine on-premise and remote work now the new norm. As revealed in the KPMG 2021 CEO Outlook, this means business leaders are ambitiously pursuing the technology and tools needed to create new work models that combine the flexibility and convenience of both approaches.

Key to this new world are seamless technology connections, coupled with a heightened focus on security. This can be supported by the use of digital identity and access management (IAM) tools. IAM is vital to enforce access controls to information (particularly when off-premise), while also supporting regulatory compliance, risk, governance, privacy, workforce lifecycle management, and enterprise-wide efficiencies.

IAM is not just useful for employee security, but is also proving to be a key differentiator when it comes to customer identification, security and experience. In the era of digital commerce, consumer identity and access management (CIAM) plays a 'concierge' role in directing and overseeing customer access to a business's digital products, while also optimising the customer experience.

Importantly, IAM tools bring the benefit of the latest in data and analytics capabilities, automation and Artificial Intelligence (AI), helping organisations to shift from reactive to proactive risk management, and gain enhanced efficiencies via informed decision making.

In today's fast-evolving ecosystems, organisations need to balance new ways of working and customer behaviours and demands with securing their information. This report explores how organisations can make the most of IAM to achieve this.

"We are living in a new world where the boundaries of our workplace, home life and leisure time are blurring. Proving who you are, securely, easily, and in whichever context you want, isn't easy. Digital identity has embraced the challenges of the modern world, and new technologies now allow authentication at the next level."

DANNY FLINT, PARTNER, DIGITAL TRUST & IDENTITY, KPMG AUSTRALIA

IAM as a critical gatekeeper

It is clear that the future of work is shaping up to be a hybrid model that combines remote and traditional workplace approaches. As reported in the KPMG 2021 CEO Outlook, global CEOs are creating a more flexible work environment that offers the convenience of working from home along with the ability to collaborate with colleagues in workplace settings. The report found:

- More than half (51 percent) of CEOs are looking to invest in shared office spaces for increassed flexibility
- 42 percent will look to hire talent that works predominantly remotely, seizing the opportunity to expand their reach into a wider pool.

Hybrid working is not an entirely new trend, however, with many organisations travelling on the path towards this for some time. This move has been enabled by evolving technology, mobile devices and internet hyperconnectivity. However, amid this increased flexibility, there have been increased security risks. These risks include:

- **Embracing the cloud:** The rapid evolution of business models has led to the relocation of applications and services from on-premise data centres to virtual cloud environments. While this enhances capability, if not set up securely, risk can open up.
- **Collaboration platforms:** The increased use of online collaboration platforms that may not be properly screened for security by the organisation.
- **Outsourcing business support functions**: As organisations have focused on optimising costs, they have increased outsourcing. In return, suppliers need remote access to systems and infrastructure, which can also open up risk.
- **Collaboration with partners:** Organisations are working more collaboratively to develop new solutions and innovations. This means giving wider access to cross-organisational data, infrastructure and assets, which could also introduce risk.

With this changed way of working and increased sharing of information, organisations are asking: How do we keep our information safe?

A sharper lens on security

Many organisations are wisely placing a sharper lens on the need for enhanced capabilities for secure data protection and access controls. Business leaders are asking, is it necessary to apply additional controls when working remotely, or can we rely on the technology that we already use? Looking at current technologies such as virtual private networks (VPNs), virtual desktops and mobile devices, are they fit for purpose now and into the future? Regardless of the platform used, it is imperative to have a higher level of assurance for identity verification of those attempting to access privileged spaces, business-critical systems, or confidential data.

IAM as a key security tool

IAM can serve as the critical gatekeeper of valuable information and resources. When designed and implemented effectively, IAM can help to mitigate remote working security risks, while helping to improve efficiency. IAM has specific features that assist with this, including:

1. **Context awareness:** IAM tools can evaluate, based on specific variables, the identities of those trying to access data. Variables such as employee location, time of day and the device used to log in are evaluated to provide a risk level. The risk level drives controls that deliver additional assurance of the user's identity. For example, an organisation could require an extra authentication factor when someone is accessing a business-critical application.
2. **Identity and access governance:** IAM can help to make sure access rights to different levels of information are granted appropriately, whether working remotely or on-premise. Governance over processes, procedures, approvals and monitoring can help IAM identify potential threats before they impact the business. This can involve assigning responsibilities and performing reviews, to make sure IAM-related incidents are not missed or identified too late.
3. **IAM to enhance security operations:** Specific security incident and event management (SIEM) tools help to monitor user activity across an organisation, but can miss the context to determine whether user activity is authorised or not. The missing context can be resolved by integrating SIEM and IAM, as IAM will enable a SIEM tool to better identify exceptions, and can also be used to deactivate access in response to a threat.

"With cyber security infringements now a prevalent risk to every business, the rise of identity as a key foundation of all security postures for business has never been more important. Identity is at the core of business success now and into the future."

MALCOLM BROAD, DIRECTOR, DIGITAL TRUST & IDENTITY, KPMG AUSTRALIA

Consumer digital trust

COVID-19 has not only increased remote working, but digital commerce as customers embrace the convenience and safety of online transactions. As a result, organisations are pursuing digital transformation and powerful new capabilities that can deliver the seamless and personalised experiences that today's savvy, hyperconnected customers expect.

Informed customers also care about digital security and privacy, and want to trust that brands are protecting both the organisation and customers. For organisations, the reverse also matters, as trust in customers is in flux due to fraudsters and attackers impersonating legitimate customers. Therefore, security and trust are not just about enterprise security, but are also about protecting customer data and carefully managing its use.

If an organisation falls short in providing a secure and reliable experience, customers may go to a competitor or new entrant that can make them feel more assured. Providing appropriate security has therefore become crucial, and CIAM is a key way to do this.

Customer security considerations

When focusing on customer digital security, three areas need consideration. They are:

1. **A new security mindset**: Historically, security has been about protecting things like money and assets, including the value of the data a business holds. When it comes to digital trust, organisations are protecting more than their data, now including the 'customer identity' itself. This involves thinking more holistically about what needs protection.
2. **Seamless interaction:** It is imperative that businesses and brands make digital interactions as simple as possible for customers. Key to this is putting the right risk tolerances and mitigations in place, while offering the user a seamless and convenient experience.
3. **An improved risk posture:** Taking customer security to the next level can be enhanced with threat analytics and sharing of data with like-minded companies. Meanwhile, organisations can warn customers if their information has been involved in a potential breach.

CIAM to build customer trust

To help organisations deliver the digital and omnichannel experiences that customers expect and will trust, while upholding their privacy and security, CIAM tools are key. CIAM tools help to direct and oversee customer access to a business's digital products and services. The quality of this 'concierge' experience can be the difference between engaging customers and alienating frustrated customers who turn to the competition to meet their needs and expectations.

To facilitate a seamless experience, federated identity models (FIMs) – which help identify individuals based on certain personal behaviours and attributes – can be used. This means an organisation can adopt another organisation's existing profile of a customer to support identity verification, as well as providing convenient online services and transactions. For example, when customers are able to quickly gain access to a service via their existing customer profiles, such as their social media profiles, it provides ease of use. The customer can quickly create a profile for the new organisation based on previously entered data, rather than re-entering their personal information. Meanwhile, organisations don't need to invest in an independent security interface, and can leverage the weight of a larger organisation's resources. This approach requires having a clear risk appetite framework.

"Identity is no longer usernames and passwords, it is a marriage between a frictionless user experience and 'zero-trust' security. Consumer expectation needs to be built on trust, consent and focused user experience."

MATT O'KEEFE, ASPAC CYBER SECURITY LEADER AND PARTNER, KPMG AUSTRALIA

Demonstrating ROI

The onset of COVID-19 saw organisations pivot quickly towards digitisation for their staff and customer service. Due to the urgency, they may have been spared scrutiny over return on investment (ROI). However, as the 'new normal' unfolds, the urgency for IT and cyber leaders to justify spending on identity solutions and demonstrate ROI will increase. A common issue is that IAM initiatives can fail to deliver on business objectives. Often IAM projects are focused on onboarding and connectivity issues, with organisations failing to prioritise risk mitigation outcomes. It is therefore important to consider key success metrics from both operational and risk perspectives.

Success metrics could include:

- The number of at-risk accounts cleaned and number of potential breaches avoided
- The reduction in help desk tickets for account management requests
- A reduction in time needed to complete access requests.

Data and analytics for decisions and governance

When implementing an IAM approach, in addition to enhanced security for workplaces and customers, the power of data analytics and automation is a core benefit. IAM-based data analytics can help with:

Anomaly detection: Identity data analytics can be used to spot and evaluate risky behaviours, such as access requests, entitlement changes, user employment status and more. Both supervised and unsupervised machine-learning approaches may be used. For example, supervised machine-learning models can analyse user-access behaviours and detect unusual activities. These could be the use of different modes of authentication, or logging in from an unexpected IP address. Meanwhile, unsupervised techniques using anomaly detection models can determine outlier behaviour based on the norm. Once risky events are identified, they can be mitigated by cleaning up excessive access rights. Other techniques to identify outliers include network graphs, peer group analysis and common roles analysis.

Account monitoring and policy violation detection: As activity data from IAM tools is generated, it can be fed into machine-learning engines, making it easier to monitor changes and better identify or predict outliers. Automated account monitoring looks for typical identity management blind spots and policy violations, for example, orphan/dormant accounts, and accounts with excessive or unused entitlements.

Analytics in identity certification campaigns: Identity analytics tools have progressed to support a 'continuous compliance mandate', using risk-based micro-certification steps. Micro-certification can be built into the identity lifecycle workflow (starting with access requests, approvals, certification campaigns, etc.), so that organisations gain insights into the types of applications and devices involved, helping reviewers and approvers to make informed and accurate decisions at pace.

Automated access rights and roles provision: AI-driven analytics are progressing toward recommending access rights and roles for users automatically. This is much like the systems being used by digital commerce platforms to recommend products and services based on previous customer purchases and products viewed. For example, if a user has exhibited patterns that don't require use of all of the access rights granted, the system may be configured to recommend that the user's access be more limited. This should minimise the risks of users having access to systems and data they should not be able to, or need to access.

Improve operational efficiency

Another compelling benefit of data analytics and automation in identity governance is the ability to increase operational efficiency. With the short supply of skilled and qualified professionals in security, combined with increasing cost pressures, chief information security officers are being asked to do more with less. As identity management lifecycle tasks such as access requests and certifications can be repetitive and error-prone, they suit automation of high-confidence, low-risk decisions. Data analytics and automation can give identity governance teams more time and resources to manage complex decisions and activities, while reducing errors.

"Deploying advanced data analytics to derive identity insights will, in addition to monitoring policy or rights violation, go a long way in identifying and addressing fraud and insider attacks. Given the shortage of skilled cyber security analysts and experts, data-driven insights solve the problem of scale and 'doing more with less'."

ANTHONY COOPS, ASPAC DATA & ANALYTICS LEADER, KPMG AUSTRALIA

The future of authentication

Currently, a great amount of identity verification is done with passwords. While easy to use, they can be problematic as the onus falls on users to remember and update them regularly. Next, multi-factor authentication mechanisms such as short message service (SMS), tokens and biometric authentication are helping to protect accounts. However, these still have shortcomings, as hackers can hijack text messages, for example. Hardware authentication devices are adding to the layers of protection available, however they tend to be expensive, can be misplaced, and hard to maintain. Finally, mechanisms such as biometric authentication are sophisticated, however, there is a chance of false negatives that disproportionately affect vulnerable communities and minorities.

As no single tool is foolproof, it is critical to move toward a 'zero-trust model' of digital identity. This is an approach to security that is fundamentally about interrogating every transaction at every connection point, in various ways, seamlessly for the user. This means that every time someone seeks access to an organisation's information, both internally and externally, the organisation can validate key identity factors: biometrics, the specific device, and user behaviours such as the location, time and frequency of access.

Portable identities

Beyond what individual organisations can do, efforts are underway to develop self-sovereign identities. These are portable representations of people's digital identities that will be proofed by governments, financial institutions, utility providers and others. With these forms of identity, consumers and citizens can choose which organisations to share them with. For example, in the US, it is possible to link one's digital travel identity to one's medical records and vaccine status, etc. However, only by public-private cooperation can organisations harness the innovation, agility and scale necessary for this to be successful.

"In 2022, we are starting to see the end to the era of the password. We embrace a digital identity ecosystem where digital authentication goes covert, using data from your trusted device, the way you use it, combined with your biometrics."

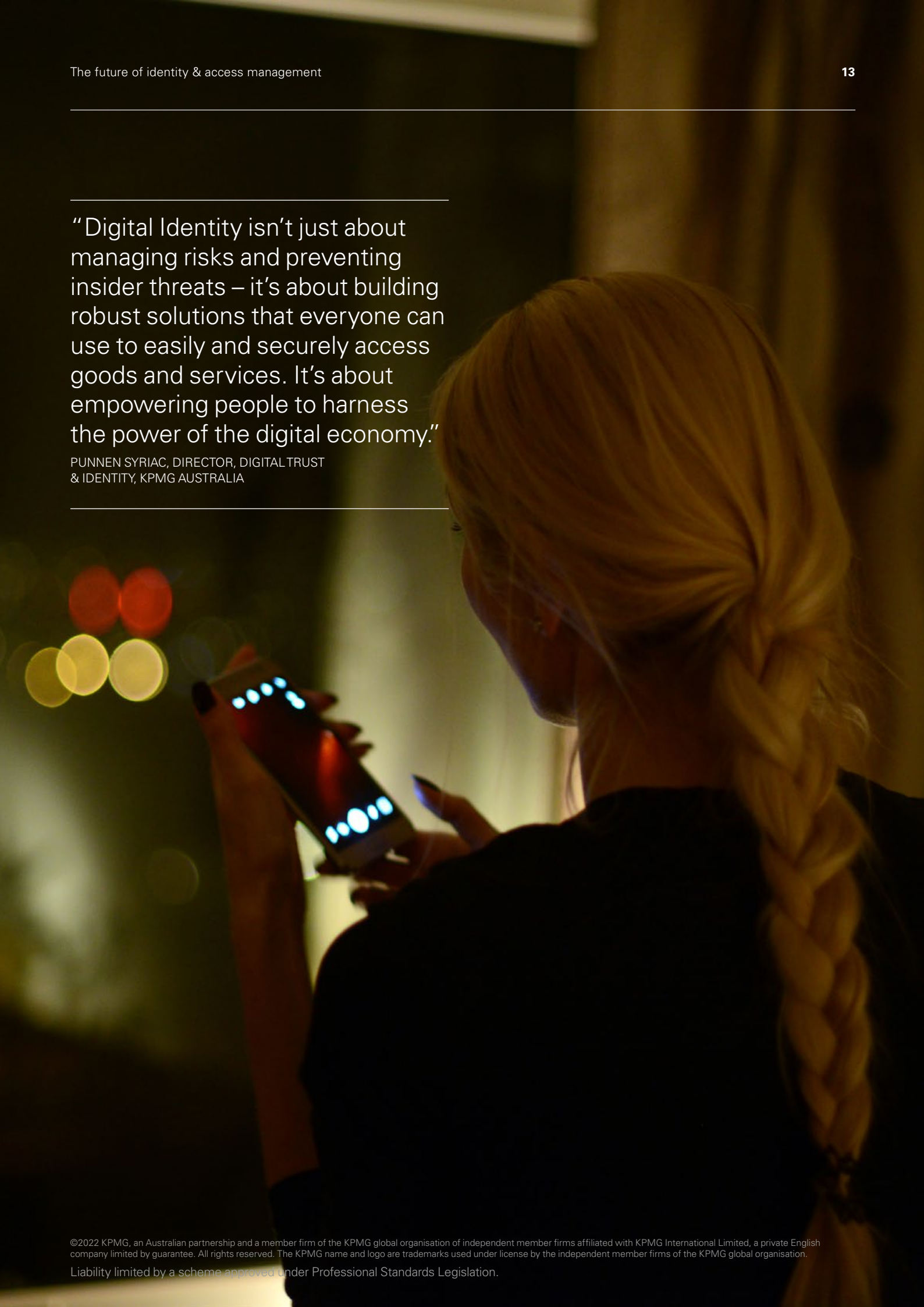
MARTIJN VERBREE, PARTNER, TECHNOLOGY RISK & CYBER, KPMG AUSTRALIA

Convergence for additional security

Typically, stakeholder groups such as the organisation and customers have used different controls, technology stacks and frameworks. A new way forward is convergence, which sees organisations treat their workforce, customers and partners similarly in the security realm. Using a common framework to manage digital identities means organisations can leverage a common set of capabilities across consumers, partners and employees.

Some tips on how to manage convergence include:

1. **Bring the internal and external together:** By making sure external fraud and internal threat programs are linked, not only does this give full visibility to all potential threats, but it makes it easier to see patterns of crime which blend internal and external vectors.
2. **Focus on monitoring capability:** For an organisation to offer relevant, timely and highly personalised experiences, it is critical to be able to detect and monitor who is doing what with digital access. Organisations are often good at authentication, but the follow-up monitoring can be a shortcoming in security programs. For example, a lack of integration with processes such as new joiners, movers and leavers can leave businesses vulnerable.
3. **Take a risk-based approach to protecting data:** It is important to know which data assets merit the highest level of protection. 'Zero-trust' approaches can provide 'fine grained' access rights – but they depend on an understanding of which information is of most value to the organisation and focusing on protecting that most.



"Digital Identity isn't just about managing risks and preventing insider threats – it's about building robust solutions that everyone can use to easily and securely access goods and services. It's about empowering people to harness the power of the digital economy."

PUNNEN SYRIAC, DIRECTOR, DIGITAL TRUST & IDENTITY, KPMG AUSTRALIA

In summary

With changes in how people work and access organisational information, along with heightened customer expectations of digital interactions, privacy and security, a robust IAM approach is essential.

As this report has explored, the benefits of IAM include increased protection of information, improved risk management, insightful data for decisions, smoother operations, and an improved customer experience among many more.

Smart, forward-looking organisations will waste no time in working towards the future of IAM, focusing on 'zero-trust' approaches for continuous protection, as well as convergence between internal and external IAM for the most holistic view of risks.

"Digital Identity is at the centre of cyber security. Trust can only be achieved if you can prove, with certainty, that the right people have the right access to the right data at the right time."

GORDON ARCHIBALD, NATIONAL LEAD, CYBER SECURITY, KPMG AUSTRALIA

Contributors

David Ferbrache, Global Head of Cyber Futures, KPMG International

Danny Flint, Partner, KPMG in Australia

Punnen Syriac, Director, KPMG in Australia

Ajit Ravi, Associate Director, KPMG in Australia

James Wilhelm, Principal, KPMG in the US

Jacob Pszonowsky, Principal, KPMG in the US

Siddharth Thakkar, Director, KPMG in the US

Diarmuid Curtin, Director, KPMG in Ireland

Ser Yen Lee, Partner, KPMG in Singapore

Contacts

Danny Flint
Partner, Digital Trust & Identity
KPMG Australia
E: dflint@kpmg.com.au
T: +61 7 3434 9191

Malcolm Broad
Director, Digital Trust & Identity
KPMG Australia
E: mbroad@kpmg.com.au
T: +61 2 9273 5056

Punnen Syriac
Director, Digital Trust & Identity
KPMG Australia
E: psyriac@kpmg.com.au
T: +61 3 8663 8063

Ajit Ravi
ASPAC IAM Lead Architect
KPMG Australia
E: aravi2@kpmg.com.au
T: +61 2 9458 1553

KPMG.com.au

February 2022 828490506CYBER