KPMG

Why digital identity is now a board-level topic

KPMG.com.au

The evolution of digital identity

As the use of data permeates almost every aspect of our lives, organisations are becoming increasingly conscious of the need for a digital identity strategy to secure and enhance both digital and real-world products and services.

In its simplest form, an identity provides a digital representation of an individual, entity or device and their associated access privileges. The primary function of Identity & Access Management (IAM) is to reduce the risk of a data breach by controlling who or what can access information assets based on defined access policies, ensuring that users do not have more access than is needed to perform a designated business function. IAM also provides an efficient mechanism for facilitating access to online products or services. The capabilities offered by IAM, when correctly implemented, can help organisations to improve business efficiencies, reduce operational costs, mitigate potential cyber risks, satisfy regulatory compliance needs and enhance user experience.

As organisations have become more conscious about the role of digital identity as both a potential risk factor and business enabler, the level of investment in sophisticated IAM tools and services has grown dramatically.

Traditionally, most organisations have viewed IAM as a function of the IT department, focused on back-office operations such as user provisioning, single sign-on and password management. In recent years; however, the growing adoption of cloud services and the proliferation of mobile devices has made IAM an increasingly critical business imperative rather than a mere function of the IT back office.

There has been a rapid increase in high-profile data breaches over the past several years, many of which have resulted from a failure to adequately enforce user access. This has not only heightened sensitivity among business executives to the potentially catastrophic consequences of a major breach but has caused regulatory mandates to become increasingly prescriptive in how businesses are required to monitor and enforce access to sensitive data.

For these reasons, there is now widespread acknowledgment that effectively managing user access is a matter of responsible corporate governance that requires a programmatic approach and methodology, elevating IAM as a board-level concern rather than just another IT requirement.

An enterprise IAM program can have a profound impact on an organisation's culture and business processes. Such programs are often politically contentious and prone to organisational bottlenecks. Nevertheless, senior executives within many large organisations now recognise the importance of IAM in addressing the risk, compliance and business needs of the modern enterprise.

Major investment drivers for IAM

Several factors are fuelling investment in enterprise IAM programs:

— Rising number, sophistication and severity of data breaches

— Increasingly stringent regulatory mandates

— Rise of cloud computing and shadow IT

— The disruptive trends in the technology landscape.

The rising number, sophistication and severity of data breaches

There are countless ways in which valuable information assets such as personal data and intellectual property can be stolen and abused. The number of attack vectors are constantly increasing, as is the severity of data breaches. With the growing involvement of hostile nation states, terrorist groups and global "hacktivist" networks, the threat landscape has become more challenging than ever. The vast resources available to malicious actors enable them to develop approaches that are becoming increasingly sophisticated in nature.

Nevertheless, the most common denominator in many high-profile breaches is a failure to enforce appropriate access controls. In many cases, such vulnerabilities exist due to poorly implemented IAM solutions and inadequate access control policies.

Additionally, many organisations are struggling to keep pace with a constantly evolving business and technology landscape while simultaneously attempting to manage the cyber risks associated with each new threat vector.

Many executives are just beginning to appreciate the nature of this challenge and the scope of the transformation necessary to mitigate cyber risks. IAM is an important part of this transformation and represents a key element in achieving a mature cyber security posture.

Increasingly stringent regulatory mandates

As data breaches become more common, driving heightened public sensitivity to cyber risks, legislators are coming under increased pressure to tighten existing regulatory regimes. For companies in heavily regulated industries such as energy and financial services, regulatory mandates are becoming more prescriptive in their approach to access controls and the need to standardise the management of digital identities.

In North America, for example, version five of the Critical Infrastructure Protection (CIP) standards regulates how power utilities control logical and physical access to sensitive systems. In the past, companies had greater ability to define their own security regimes. Now they must demonstrate how they control who can access what systems and facilities. Failure to comply can lead to the imposition of punitive fines.

In financial services, regulatory authorities are becoming equally prescriptive in their approach to access management. The Financial Industry Regulatory Authority (FINRA) in the US requires financial brokers and dealers to consider certain guiding principles and effective practices in their cybersecurity posture, and evaluates their adequacy in considering the potential risk to investors and customers.

It is now common for auditors and regulators to prescribe the use of IAM solutions to remediate findings relative to user access. A common use case involves the need to identify users who may be able to compromise sensitive information assets having accrued inappropriate or toxic combinations of access privileges. Such risks can be mitigated with the use of commercial products that control privileged access, monitor usage of critical systems and perform ongoing analysis of privileges to identify high-risk users and potential Separation of Duty (SoD) violations.

The rise of cloud computing

Cloud computing has led to a major re-evaluation of how organisations manage user access. With so many corporate information assets now residing outside the traditional enterprise firewall, the notion of perimeter security is rapidly becoming obsolete. This paradigm shift is driving a heightened emphasis on IAM solutions that restrict access by controlling user privileges, credentials and permissions, leading many experts to proclaim that identity is the new perimeter.

Cloud computing has also introduced additional operational risk and complexity for organisations. Because cloud services can usually be deployed without the need to engage IT, business areas can potentially circumvent the access policies, controls and risk assessments that are typically applied when deploying on-premise solutions.

In many cases, organisations have deployed on-premise IAM solutions that control access to enterprise systems but may not have been extended to cloud services. The challenge for such organisations is to govern access to cloud systems in the same manner as on-premise systems without inhibiting the business. This requires strict governance around the adoption of cloud services and the enforcement of controls to ensure consistency with established security policies and standards.

To address these needs, many commercial IAM vendors have now developed sophisticated capabilities that extend the management of digital identities to the cloud.

Disruptive trends in the technology landscape

Cloud computing is just the first in a series of disruptive trends that are also changing how organisations approach the topic of digital identity. Five of the most significant trends are:

1. Mobile internet access
2. Digital workforce
3. Identity convergence
4. Big Data and Analytics
5. The Internet of Things (IoT).

Like cloud computing, each of these trends is fundamentally changing the ways that organisations deliver products and services and have an impact on how organisations manage user access.

1. Mobile internet access

The growing adoption of 'Bring Your Own Device' (BYOD) policies and the consumerisation of IT increasingly requires organisations to permit users to access enterprise systems using any device from any location.

Over the past 15 years, there has been a huge paradigm shift in how workers access enterprise systems. As recently as the early 2000s, most employees would come into an office every morning, log onto a workstation, do their work, and then log off in the evening before going home. Key personnel may have had a company issued laptop with VPN access to certain enterprise systems, but such cases were rare. Access to systems and data was tightly controlled, with most applications residing behind a corporate firewall.

The increased usage of non-standard devices such as smartphones and tablets over the past decade has reduced the amount of control that organisations have with regards to how employees access enterprise systems. This is particularly true of cloud-based systems that reside outside the firewall.

Additionally, some organisations now support the use of third-party digital identities and credentials to access systems. This model is known as Bring Your Own Identity (BYOI) and is commonly used to authenticate customers and other non-employees such as suppliers, contractors or business partners.

While BYOD and BYOID policies can improve user experience, convenience and productivity, they also create new threat vectors for malicious actors to exploit; for example, the possible theft of devices that contain sensitive corporate data.

Such threats have led to an increasing convergence of IAM and Mobile Device Management (MDM) solutions that conflate access policies for both people and devices. The incorporation of device-based identity management into existing IAM processes allows organisations to provide and revoke access to a mobile device as quickly and easily as they can for the employee using it.

2. The digital workforce

The rise of outsourcing, offshoring and other flexible labour arrangements has led to many workers residing outside of the corporate network.

IAM solutions are now increasingly required to control non-employee access to enterprise systems. A common approach to this requirement involves the use of federated identities, where credentials belonging to one system are relied on by another, which simplifies the process of gaining access but can introduce new complexities and risks.

Not only are remote workers located outside the corporate network, but they often use a different set of business processes, compounding the risk to organisations. In many cases, they also operate across national boundaries, which creates additional complexity because of differing and often conflicting laws and regulations in each jurisdiction.

The challenge for the modern enterprise is to enable the rapid onboarding and offboarding of mobile workers and grant the access they need without impacting their productivity or ability to do their jobs. Many organisations have attempted to use existing or legacy IAM tools to address these challenges, only to find that the risks and costs of this approach are often much higher than expected.

3. Identity convergence

As the number of digital identities continues to proliferate, organisations are faced with the challenge of how to manage access for users who traverse population siloes.

In the higher education vertical for example, it is common for the same individual to be both a student and a professor at the same university, and to require different levels of access based on the context in which they are acting. The new economy is also blurring the line between creators, users and owners of content, and a single individual may fit multiple categories.

In the past, standalone IAM solutions servicing different user populations could coexist with relatively little risk of significant overlap.

In the new digital business environment; however, an individual's access needs may be more contextual. This can be handled by using different "personas" that are linked to the same identity, with each persona having unique accounts and privileges.

Such an approach both enhances user experience and promotes a unified view of access to enforce security policies. This is only possible; however, if organisations adopt a holistic, rather than a population-centric approach to IAM.

4. Big data and analytics

As more systems rely on digital identities, advances in big data and analytics enable organisations to derive detailed intelligence regarding user access. This extends beyond the privileges and preferences of users to their access characteristics, such as geo-location, usage patterns and biometric data. Increasingly powerful compute capabilities now enable IAM solutions to perform real-time analytics that apply sophisticated algorithms to evaluate potential risk when authenticating users to information assets.

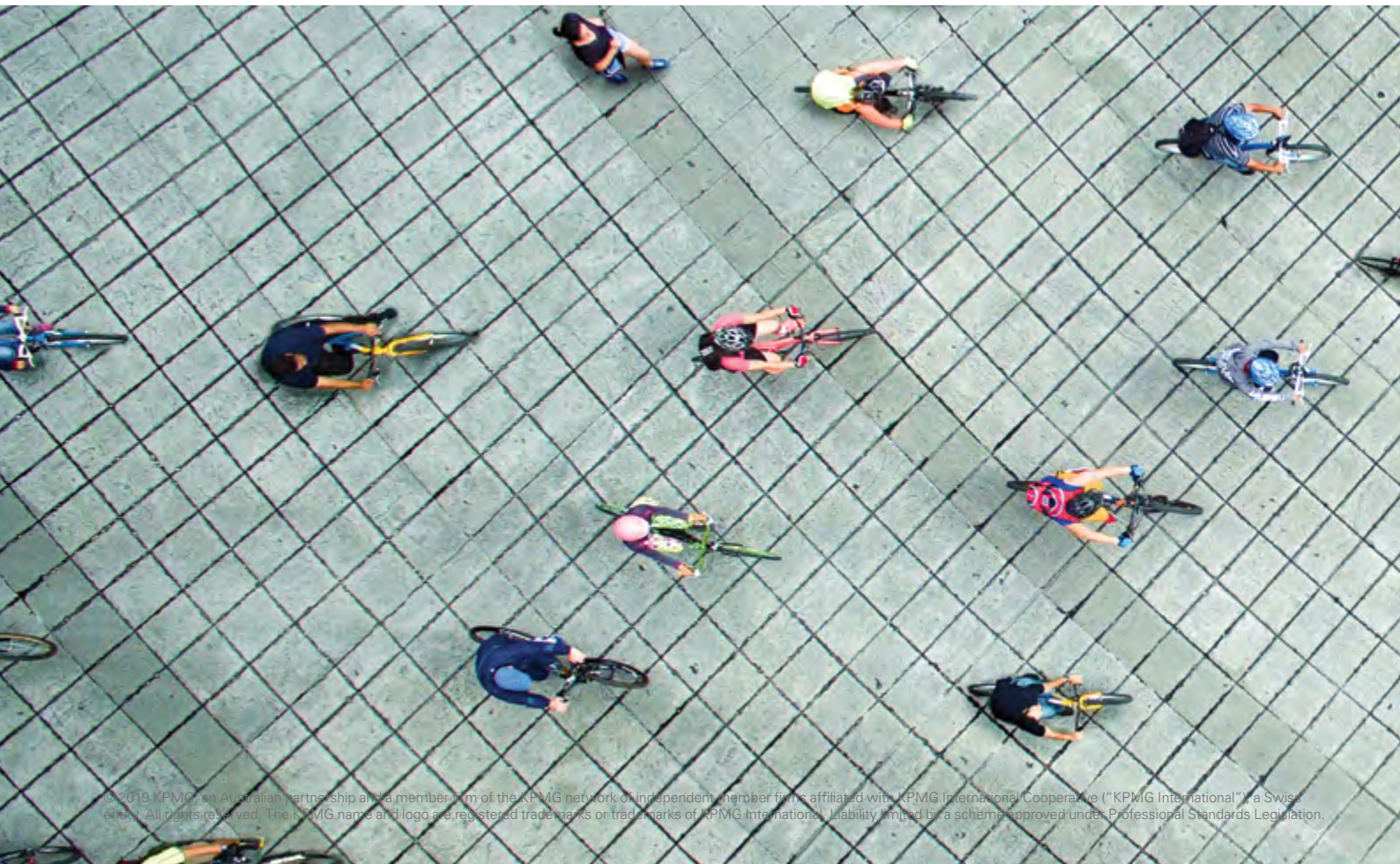
An emerging trend in IAM involves the emergence of behavioural analytics to manage user access. Additionally, there are a number of biometric factors that can be leveraged to authenticate users. These factors include voice recognition, facial recognition, fingerprint analysis, typing patterns, and even the angle at which a user typically holds their phone.

While immensely useful, this intelligence has a cost. Some organisations are compiling gigabytes of data for each user every month. Obviously, such data has to be stored in a secure fashion.

Such capabilities not only mitigate risk but also improve user experience. While a bank, for example, may use risk-based algorithms for fraud detection, they can also simplify the process of authentication for customers.

The benefits of such approaches apply equally to both enterprise and external users, which creates a powerful business case for a singular enterprise-wide identity risk platform that services all user populations.

Big data can also help to consolidate identity stores. Traditionally, employee and consumer identities have been managed separately, largely because enterprise IAM products could not easily scale to handle larger external populations. Those populations can now be consolidated into a single authoritative source based on a common schema for how digital identities are represented, irrespective of user type.



5. IoT

IoT has led to the emergence of a new form of digital identity, known as "device identity", to control how devices and automated processes transact independently within digital ecosystems.

The complexities of this new environment are only just coming into focus, arguably making it the most disruptive trend now challenging how organisations perform IAM. Early adopters are only just beginning to deploy solutions that are transforming the concept of digital identity.

When a device is assigned a unique identity, it is not just to manage or control the device itself. The device also needs to be able to transact with other devices and services in a similar way to a human user.

For example, consider an energy company with contractors in the field reading internet-connected smart meters. These devices are effectively punching holes through the energy company's firewall to their most sensitive systems. Each worker on the crew also has their own mobile device that may need to interact with smart meters and the energy company's internal systems. All of these entities need to have their own credentials, and the energy company's IAM platform needs to know who has what device, what they have access to and what they are doing with that data.

A typical consumer device, like a fitness device, operates within an even more complex ecosystem. Digital identity controls not only the device but what internet services it is connected to — including third- and fourth-party services — and what information it shares with those services based on the preferences and authorisations of its owner. As organisations seek to leverage IoT and differentiate themselves from competitors by offering superior privacy protection, security and user experience, more sophisticated IAM solutions are required.

IoT exemplifies the accelerating rate at which the IAM landscape is evolving to address the access needs of disruptive technology.

Identity-related impacts to the business

Cloud computing and each of the disruptive trends described above present three major identity-related impacts to the business: risk, inefficiency and user experience. As these trends become mainstream, their impacts will have an increasingly negative effect on business operations. Many organisations are reaching the point where effective and efficient IAM solutions cannot be implemented in a silowed fashion, necessitating a more holistic enterprise strategy that requires board-level involvement.

Risk

From a board perspective, the consequences of an identity-related breach include:

— Potential legal liability

— Brand damage

— Theft of intellectual property and sensitive information.

While the costs associated with these outcomes may appear qualitative rather than quantitative, several studies have quantified the average cost of a data breach. These are supported by numerous documented accounts describing the cost to organisations that have suffered catastrophic losses.

The 2016 Ponemon Cost of Data Breach Study, which analysed the experience of over 380 organisations around the globe, found that the average consolidated total cost of a data breach was US$4 million. The study also reported that the average cost incurred for each lost or stolen record containing sensitive and confidential information was US$158.

The 2007 data breach at a major US retailer reportedly cost the company upwards of US$4.5 billion, based on estimates of US$100 per stolen record and calculations of expenses such as legal costs, damages and a drop in sales following the breach.

Inefficiency

Because digital identity underpins the adoption of many disruptive trends, organisations will incur inflated operational costs if their IAM processes are inefficient or outdated. This often occurs when organisations attempt to apply legacy processes to evolving business and technology needs. A major shortcoming for many organisations is when legacy IAM processes and tools are used to address use cases for which they were not originally designed.

For example, a corporate IAM solution designed to manage employee populations numbering in the tens or even hundreds of thousands may struggle to handle millions or tens of millions of customer identities.

Organisations may also implement new IAM systems to meet emerging identity-related challenges. This often creates redundant operational functions that inflate operational costs, even though many of these costs may be hidden.

Many businesses already have multiple IAM tools. Some larger organisations have deployed a variety of IAM products in response to various tactical issues. These systems often overlap and conflict, creating further inefficiencies, reducing their effectiveness and increasing licensing costs.

In most cases, executives from each business area will probably have completely different perspectives on their most critical identity-related challenges. Elevating the conversation to address IAM in a more strategic fashion provides an opportunity to address these challenges holistically. Implementing an integrated IAM solution that conforms to a holistic strategy creates greater opportunities to drive down costs by optimising business processes and making them more reflective of the new business and technology landscape.

User experience

The impact of IAM on user experience is more difficult to quantify, although in some cases the cost of poor experience is obvious. If a new employee has to wait several weeks to get access to all the information they need, for example, their salary is effectively wasted, incurring unnecessary costs to the business.

Most of the time, the impact of poor user experience is hidden. As organisations adopt one cloud service after another, users often acquire multiple identities for each of these services. Without a corporate-wide approach to adoption, many organisations end up back where they were in the 1990s when it was common for each system to have its own user repository, and require users to maintain multiple IDs and passwords.

Without a holistic approach to IAM, the risk, inefficiency and user experience impacts are multiplied as additional disruptive trends impact businesses. It is not surprising that among early adopters, particularly larger organisations, the rate of technology transformation has been running ahead of corporate governance processes.

At the board level, there is both a fear of the lack of control and a growing concern about how the business can manage the risks incurred by the adoption of new technology. In North America in particular, there is currently less emphasis on IAM investments that focus on user-facing capabilities such as provisioning automation and single sign-on, and a heightened focus on compliance and risk reduction.

Adopting an enterprise-wide approach to IAM

Senior executives are becoming aware that in the modern enterprise, there are significant risks, costs and inefficiencies incurred by a siloed or departmental approach to IAM. Accordingly, discussions about IAM are increasingly taking place at the board level.

In many cases, these discussions are occurring within organisations that already have an existing IAM platform. These organisations are often challenged by disruptive trends that are transforming outdated notions of digital identity.

There is also a growing awareness of how IAM can support business transformation. Accordingly, many board-level discussions about digital identity are focused on how core IAM capabilities can enable the assimilation of disruptive trends in the digital economy.

Mergers and acquisitions may also necessitate the integration of new user and/or customer populations that are beyond the capabilities of existing IAM solutions.

Preparing for identity transformation

Because IAM can potentially impact every aspect of an organisation's technology infrastructure, business processes and user community, such programs are notorious for being politically contentious and should be viewed as an ongoing transformation program that is comparable to Enterprise Resource Planning (ERP) in terms of scope, impact and complexity. Accordingly, sustained executive backing is critical to avoid organisational bottlenecks and resistance.

The most successful IAM programs are characterised by the existence of a robust governance framework and a holistic, enterprise-wide approach to managing digital identities. This requires a well-defined change management process, beginning with an enterprise-wide communication and outreach effort designed to promote awareness and encourage participation from key system, data and process owners.

Another critical consideration for successful IAM programs is avoiding disruption to the business. This is typically achieved not by ripping and replacing existing IAM tools and processes in a "big bang" manner, but by adopting a phased and pragmatic transition to a clearly defined future state. A phased approach also enables the business to achieve quick wins, generate momentum for new phases and to make necessary course corrections as business and technology needs evolve throughout the lifecycle of the program.

To help organisations plan for this kind of transformation, KPMG member firms offer various comprehensive IAM strategic planning services such as maturity assessments, business case development, business process modelling and optimisation, gap analysis, technology evaluation and selection, strategy roadmap creation, change and communication planning and executive advisory workshops. All of these services map to KPMG's market-leading IAM reference framework, which reflects leading practices for structuring enterprise IAM programs and the emerging business and technology trends discussed in this paper.

KPMG Cyber Security Services includes a global team of seasoned IAM technology professionals who have successfully implemented enterprise identity solutions for some of the world's largest organisations.

When combined, KPMG's strategic planning and implementation service offerings cover the full lifecycle of an IAM program, enabling KPMG firms to serve as allies to clients from ideation to production hand-off.

Conclusion — IAM is a way of life

IAM is not just a technology or a tool, and neither is it a project with a defined duration. It is often a multi-year transformation program that requires sustained commitment from executives. Even once implemented, IAM solutions require constant care and feeding in order to adapt to constantly evolving business needs. Put simply, IAM is a way of life.

In the modern business environment, organisations are continuously onboarding new populations and adopting new technologies. Without a well-defined operating model and supporting governance framework, IAM solutions can quickly become outdated with a diminishing return on investment and increased risks to the organisation.

As the business and technology landscape evolves faster than ever before, risk vectors continue to proliferate and regulatory mandates tighten in response. IAM is no longer an IT problem; it is rapidly becoming a corporate governance imperative.

Contacts

Gordon Archibald
National Lead
Cyber Security Services
KPMG Australia
E: garchibald@kpmg.com.au

Danny Flint
Director
Digital Trust and Identity (Brisbane)
KPMG Australia
E: dflint@kpmg.com.au

Sim Yap
Associate Director
Digital Trust and Identity (Sydney)
KPMG Australia
E: syap1@kpmg.com.au

Punnen Syriac
Associate Director
Digital Trust and Identity (Melbourne)
KPMG Australia
E: psyriac@kpmg.com.au

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates.

KPMG.com.au

August 2019. 381547616MC.