



Conquer security threats and ignite innovation

Cyber security puts a protective arm around the day-to-day operations of your business.

KPMG Powered Enterprise | Cyber

home.kpmg/poweredyber



Cyber serenity

Cyber security risks are mounting, and the cyber security function has the potential to offer more than just a defensive strategy.

By transforming the cyber security function, organisations can reap benefits beyond the protective layer of the business by also safeguarding its digital assets and reputation.

“It’s important that businesses have the ‘cyber serenity’ to adapt to changing conditions with confidence,” says Gordon Archibald, National Lead, Cyber Security, KPMG Australia. “When organisations weave cyber security into the fabric of their business, they can protect critical assets, win trust and confidently seize opportunities.”

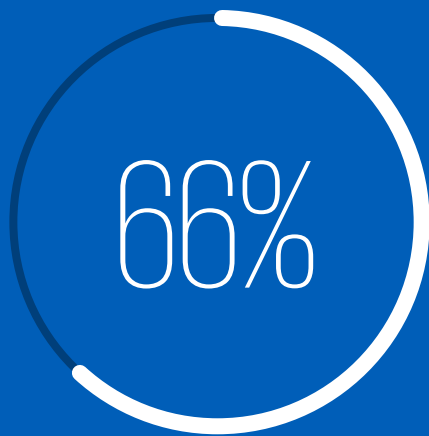
Effective identity and access management (IAM) and security operations (SecOps) serve as a foundation for cyber security programs, and the importance of a leading cyber security function increases day by day.

Technology is an integral component of almost every business, and cyber security is there to protect the future.



The cyber security challenge

For most companies, a security monitoring function of some description is a given. However, it is often a costly and reactive solution.



of digital transformation leaders plan to **increase investments in data security** measures in the next 12 months.

Base: 820 professionals involved with digital transformation strategy decisions

Source: A commissioned study conducted by Forrester Consulting on behalf of KPMG, April 2021

It's a familiar story in many organisations of all shapes and sizes across the globe: technology solutions have been implemented across siloed departments to solve an existing and discrete problem.

"In a lot of cases, businesses are detecting threats too late, or postmortem following a breach response," says Danny Flint, Partner, Digital Trust & Identity, KPMG Australia.

"They identify opportunities to improve monitoring in the future, but they don't have a solid strategy around how they are going to deploy and implement those improvements. They haven't wrapped the right people around the technology. They've just turned it on, and it's often not effective at detecting threats. So they are spending a lot of money for limited risk reduction."

The consequence is a patchwork of technology with variable levels of security and little integration – often at great expense.

"Businesses are using so many different tools, and ineffective methods of tracking such as spreadsheets and emails, that many don't even know what their weaknesses and vulnerabilities are," says Flint.

While the importance of security operations (SecOps) is increasingly well understood, identity access management (IAM) is a niche component. As its gravity isn't always appreciated.

Managing identity access across a multitude of software and systems – both from the internal enterprise and external consumer perspective – is a significant challenge.

Get it right and it's the first line of cyber defence. Get it wrong and it's an open door to a would-be attacker.

"The transformation of identity access is sometimes viewed as too complex," KPMG Australia.

"However, there are practical answers. The structured KPMG Powered Enterprise | Cyber transformation for example, is a proven methodology to change the way enterprises handle and transform identity management, and it guarantees efficiencies while improving overall security."



One of the critical areas of IAM focus from an enterprise perspective is around joiners, movers, and leavers. Typically this has been managed inconsistently in onboarding people, issuing and recording permissions, and removing the credentials of people who've departed the business. Too often as employees change roles, they keep their existing permissions and that can lead to an accumulation of out-of-proportion access to highly sensitive data and applications.

From a consumer perspective, IAM is focused on ensuring that the customer's identity is as protected as possible and guarded against malicious activity, without compromising the ability to access services. The customer experience is as crucial as the security aspect of identity management.

In a recent example, the onboarding process for a university to move potential students from the offer of a place to acceptance required creating an

account that included 28 people, each of whom had a different role in the process. It could take more than seven days to create an account, and during that period, 25 percent of prospective students typically dropped out.

This process was transformed by Powered Cyber; a four-stage process was introduced, enabling accounts to be opened within 40 minutes. The dropout rate of 25 percent was immediately reduced to five percent.

To achieve that level of efficiency, a new leading-practice operating model is required.

Turning risk into competitive advantage

A transformed cyber function can be a springboard for innovation and can deliver an enviable level of trust, both with customers and clients at an enterprise level as well.



“Everybody looks at risk – of which cyber is a component – as a cost centre,” says Tims. “But good cyber security can bring a strong competitive advantage.”

A new operating model with a proactive and forward-thinking approach to cyber can transform an organisation’s cyber security function, building trust throughout the enterprise and its customers.

By identifying skills gaps and modeling the organisation’s maturity around its operations, organisations can embed new ways of working, delivering change across the enterprise to support and sustain high performance.

From a SecOps perspective, a threat assessment or threat profile is performed to identify the threats and the preventative controls an organisation has in place.

The results are then balanced against the threat actors that are likely to target them, why they are likely to be targeted and how these threat actors would operate. When you bring these components together, it shows the most significant potential risks for the business.

By implementing holistic technology across the business, the cyber security unknowns are significantly reduced, if not eliminated, engendering greater confidence levels from internal and external stakeholders alike.

When it comes to IAM, it’s critical to understand who is accessing different systems and why.

“A strong identity system needs multiple data points to build trust about the person who’s accessing the system,” says Flint.

Some of those authentication factors are obvious – for example, device type, location, browser version. Increasingly, however, more complex elements are being added: biometrics, impossible travel, behavioral patterns (such as how an individual swipes), usual time of log-on. Incorporating a variety of authentication factors makes it more difficult for threat actors to take over credentials.

Implementing this level of cyber security is a crucial step towards changing the perception of cyber from a protector to a proactive, strategic contributor to the business.

Cyber security can be proactive and reduce the amount of time spent on ‘protection’ by minimising weaknesses and using validated technology solutions with proven real-world usability to automate many mundane day-to-day tasks.



Everybody looks at risk – of which cyber is a component – as a cost centre...but good cyber security can bring a strong competitive advantage. ”

Mark Tims

Partner, Technology Risk and Cyber,
KPMG Australia

Don't just manage risk. Master it

Thanks to preconfigured cloud technologies, processes and organisational designs, tailored to unique businesses, Powered Cyber is designed to significantly accelerate the delivery of IAM and SecOps programs.



Transformation of the cyber function focuses on delivering business outcomes that combine the 6 layers of the **KPMG Target Operating Model**: functional process, people, service delivery model, technology, performance insights and data, and governance.

“The TOM helps businesses to change, to implement proven leading practices, to fast-track transformation and keep it on course,” says Verbree.

Once a new operating model is established, businesses can expect a range of business outcomes, including:

SecOps

1. **End-to-end views of Security, IT and Governance, Risk, and Compliance:** Drives end-to-end risk-management processes across the organisation through automated security control testing and enhanced reporting of risk and compliance posture.
2. **Faster, integrated and standardised response:** Who does what, why and how. Identifying the skills, roles, and responsibilities your business requires.
3. **An accurate view of current security posture:** Where the work gets done, shared service centre, centres of excellence and outsourcing operating models to optimise service delivery.

IAM

1. **Control of user access to applications, systems, file shares and sensitive data:** Manages user access across the business, gaining efficiencies through policy-driven access control rules both on premise and in the cloud. Significantly reduce the risk of "insider threat" by applying the principle of "least privilege".
2. **Improved quality and effectiveness of reporting and analytics to support decision-making:** Feeds real time user access data to Risk and Security Information and Event Management (SIEM) systems, reducing the risk of systemic malicious activity
3. **Automate processes to reduce reliance on IT:** Achieves efficiency – for example, access requests, lifecycle management events, certification campaigns, password management.

“Businesses can immediately benefit from deep IAM and SecOps knowledge, and quickly achieve security operations transformation in the cloud,” says Flint.
“Powered Enterprise is an outcome-driven transformation solution that drives sustainable change, rising performance and lasting value.”

Cyber at the heart of the business

By jumpstarting the digital transformation of the cyber function, businesses can take advantage of leading best practices with reduced implementation risk and a quick time to value.

In addition, a trusted cyber function can be the springboard for new business activity. From product launches to acquisitions and mergers, having a robust and proven cyber function provides the confidence and reliability needed to seize opportunities and respond to market challenges quickly, efficiently and effectively.

With optimal confidence in cyber capabilities both internally and externally, cyber can genuinely be a strategic business partner and value contributor rather than a reactive security effort.

And for a business that's going to flourish over the coming years, that's exactly what it needs to be.



Key takeaways

1. **Cyber is a fundamental part of a business**, not just a tick box.
2. When organisations weave cyber into the fabric of their business, **they can protect critical assets, win trust and confidently seize opportunities.**
3. Effective identity and access management (IAM) and security operations (SecOps) **serve as a foundation for cyber security programs.**
4. A proactive and reliable cyber function gives **stakeholders and other departments the confidence to execute their roles effectively.**
5. **Powered Cyber drives transformation in your business**, allowing you to more effectively use identity technology to protect your assets and enforcing industry-leading security.

Discover more

How Powered can help:

- 🔗 **KPMG Powered Enterprise**
- 🔗 **KPMG Target Operating Model**

Insights from KPMG:

- 🔗 **Connected. Powered. Trusted.**
- 🔗 **Cyber Security Insights**

Contact us today:

Danny Flint (National Partner)

Digital Trust & Identity

T: +61 410 752800

E: dflint@kpmg.com.au

Punnen Syriac

Digital Trust & Identity (VIC)

T: +61 403 282583

E: psyriac@kpmg.com.au

Malcolm Broad

Digital Trust & Identity (NSW)

T: +61 406 533 587

E: mbroad@kpmg.com

Jacques Swanepoel

Digital Trust & Identity (QLD)

T: +61 410 036 168

E: jswanepoel1@kpmg.com



KPMG.com.au

The information contained in this document is of a general nature and is not intended to address the objectives, financial situation or needs of any particular individual or entity. It is provided for information purposes only and does not constitute, nor should it be regarded in any manner whatsoever, as advice and is not intended to influence a person in making a decision, including, if applicable, in relation to any financial product or an interest in a financial product. Although we endeavour to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act on such information without appropriate professional advice after a thorough examination of the particular situation.

To the extent permissible by law, KPMG and its associated entities shall not be liable for any errors, omissions, defects or misrepresentations in the information or for any loss or damage suffered by persons who use or rely on such information (including for reasons of negligence, negligent misstatement or otherwise).

©2021 KPMG, an Australian partnership and a member firm of the KPMG global organisation of independent member firms affiliated with KPMG International Limited, a private English company limited by guarantee. All rights reserved.

The KPMG name and logo are trademarks used under license by the independent member firms of the KPMG global organisation.

Liability limited by a scheme approved under Professional Standards Legislation.

November 2021, 775232724FIRM.