KPMG

Seizing opportunities to build business value

KPMG Cyber Security
services and capabilities

KPMG.com.au

It's time to view cyber security as a business strategy

It's no surprise that cyber security continues to be a key area of focus for today's organisations. What's changing is how top business leaders view cyber. For many, it's no longer just an IT issue, but a critical part of their overall business strategies.

According to KPMG's 2018 CEO Outlook Survey, there is acknowledgement of the importance of a strong cyber strategy. Two-thirds (66 percent) agree that this is critical to engender trust with key stakeholders, while 68 percent view customer data protection as one of their most important personal responsibilities, enabling long-term growth of the customer base.

The 2018 Harvey Nash/KPMG CIO Survey, the largest IT leadership survey in the world, found almost a quarter more respondents than in 2017 are prioritisng improvements in cyber security as cyber crime threats reach an all-time high. Protecting the business from a cyber attack has jumped further up the boardroom agenda than any other item and IT leaders are being supported and encouraged to make their defences the best that they can be.

Today's leaders increasingly understand that by adopting this new strategic perspective, they can expand the value of their cyber security efforts – from protecting critical assets to embracing new business opportunities and improving their competitive advantage.

But this transformation takes a clear strategy and expert insight to understand, prioritise and manage cyber security risks. With cyber security under control, you can reduce uncertainty, increase your agility, and turn risk into advantage.

"If a cyber program is too rigid or structured to deal with the types of changes that we expect modern companies to face, then it can be an encumbrance rather than an enabler. You need an enterprise cyber program that is strategically aligned and supports business strategy and outcomes."

Gordon Archibald,
Partner, Cyber Security Services, KPMG Australia

Seeing cyber security through the lens of your business

"As businesses become more digitised, automated, data driven and move into the cloud, strong cyber security will become one of the core foundations that will underpin success."

Mark Tims,
Partner, Technology Risk,
KPMG Australia

It's impossible to compete effectively in today's global marketplace without embracing digital information and emerging technologies. Yet, this can also make your organisation more vulnerable to cyber risk. The question becomes, how do you take advantage of these powerful business tools, while protecting your critical data assets?

At KPMG, we believe the best approach to cyber security is one that delivers value by:

- protecting your critical assets
- enabling your business strategies
- providing resilience for sustainable business growth.

This starts by recognising that different organisations have different challenges, and different appetites for risk. Our team can work closely with you to help determine which risks you can accept and which you need to manage.

We base our approach on your company's strategy and on the insights we gather from asking questions like:

- What kinds of threats would cause the greatest harm to your business today?
- What data do you rely on for mission-critical processes?
- How can embedding cyber security strategies into your products and services give you a competitive advantage?

This results in a new perspective on cyber security. One that provides you with strategy, processes and technology to manage your cyber security issues, and allows you to replace uncertainty with confidence and agility as you pursue new opportunities.

Defend, enable and maintain your business

Organisations agree that cyber resource and investment allocations must be balanced among traditional reactive safety measures, more proactive business enablement, and advanced sustainability objectives. That is, they must defend, enable, and maintain their business.

Cyber Defence

Includes actions and infrastructure intended to defend the perimeter, protect sensitive data, and thwart malicious attackers, which involves pre- and post-breach activities.

Business Enablement

Involves cyber teams working collaboratively with business owners to achieve growth and strategic objectives (e.g. digital transformation), allowing the business to grow at its own pace while aligning to security policies.

Resilience

Represents an organisational commitment to cyber maturity, enablement, and integration; which involves business, financial and cultural alignment to security, process automation and technical automation.

"Balancing opportunity and threat is a complex challenge for organisations as they adopt new digital disruptive delivery models. Our strategy, governance, and transformation capabilities assist clients in aligning the cyber agenda with their dynamic business strategies and compliance requirements, enabling a governed state of managed cyber risk."

Jeremy Dunn,
Strategy and Governance Lead,
KPMG Australia

"The use of GRC technologies is a fundamental enabler in efficiently aligning cyber governance, risk and compliance functions to the organisational strategy, allowing for convergence and transparency of information, driving increased performance and operational resilience in a rapidly changing world."

Max Drabik,
Cyber Governance,
Risk & Compliance Lead,
KPMG Australia

Our range of Cyber Security services

KPMG looks at the world from your perspective, bringing a business context to cyber security for all levels of your organisation – from the boardroom to the back office.

This begins with helping you understand, prioritise, and manage your cyber security risks through four distinct capabilities that take you from strategy through implementation.

Strategy and governance

This set of services is designed to help clients understand how best to align their cyber agendas with their dynamic business and compliance priorities —including risk management. Among the approaches we follow are: assessing cyber maturity and compliance, providing reports and metrics to chief information security officers (CISOs), and more.

Cyber transformation

We help clients fulfil their cyber agendas by building and improving their programs and processes. This is accomplished through support by the right organisation and technology, and includes identity and access management (IAM), security governance, risk management and compliance (GRC), and other services.

Cyber defence

KPMG's cyber defence professionals help clients maintain their cyber agendas as their business and technology programs evolve. We do this by providing greater visibility and understanding of changing risks through such processes as technical assessments and security operations and monitoring.

Cyber response

These services are designed to help organisations respond to cyber incidents effectively and efficiently, as well as conduct forensic analysis and detailed investigations. Among the specific areas these cover are incident response readiness and planning and digital investigations and remediation.

Strategy and Governance

- Cyber Maturity Assessment (CMA)
- Business Resilience/Crisis Management
- Privacy Readiness
- Third-party security risk management
- CISO as a Service
- Target operating model development
- SWIFT assessment

Transformation

- Identity and access management (IAM)
- Security GRC
- Federal Hosted
- Cyber strategy/target operating model development
- Cyber Assurance

Cyber Defence

- Digital – IoT, Blockchain, mobile, cloud security
- Technical assessments
  - Applications
  - Network
  - Infrastructure
- Cyber Security architecture
- SCADA/ICS assessment
- Threat Hunting
- Security operations design

Cyber Response

- Incident response readiness and planning
- Digital investigations and remediation
- Threat intelligence
- Sensitive Data Finder

"In Cyber Defence, we think like the bad guys and provide a true-life assessment of cyber risks. We use our practical insights and hands-on technology experience to help our clients design and architect security capabilities, develop and deploy solutions that are secure by design and help improve their overall resilience to cyber-attacks."

Priyank Baveja,
Technical and Architecture Lead

"Effective Cyber Response stems from an integrated approach combining an existing understanding of our clients environment with a rapid response capability established through on call agreements. This framework allows us to focus on pinpointing the issue and minimisation of its impact by having the right resources, with the right skills rapidly deployed alongside our clients during a breach."

Stan Gallo,
Partner,
Forensic

Why KPMG

KPMG brings a business context to cyber security for all levels of your organisation — from the boardroom to the back office.

We know cyber security is a business issue, not just an IT issue.

Cyber security is a strategic enterprise risk that goes far beyond IT. Uncontrolled, it can impact product integrity, the customer experience, investor confidence, operations, regulatory compliance, brand reputation and more. That's why cyber security demands attention not only from the chief information officer, but also from rest of the C-suite, the board, employees and business partners.

We translate cyber security into a language your business can understand.

Cyber security affects different parts of your business, and we translate cyber risks into an appropriate language for each. Whether we're working in your boardroom, back office or data centre we seek to provide a jargon free explanation of your cyber threats, the potential impact to your critical assets and the recommended responses.

We provide a business-led approach, supported by deep technical skills.

We bring a combination of technical domain expertise and cross-functional business expertise, including People and Change, Financial Management, Risk Management, global compliance, organisational design and more. KPMG professionals understand cyber security risks in all layers of your business so we can advise you in a context that's relevant to you.

We work collaboratively with you to meet your cyber security needs.

Instead of coming to you with a preconfigured approach, KPMG professionals take the time to understand your business priorities, strategic direction and operations. This means we can bring an appropriate context to your cyber security risks and help protect your critical business processes.

We know your industry.

As you're navigating cyber security, it's important to have an advisor at your side who understands the challenges, threats and strategies in your industry. At KPMG, we bring both the business context and the industry context to cyber security. Leveraging the industry experience of KPMG professionals around the world, we understand where your industry is coming from in cyber security, and where it's going.

We help you from the boardroom...

Putting cyber security on the board's agenda is critical in adopting a holistic strategy. Because we understand the business issues, challenges and concerns facing today's senior management and boards, KPMG can help you start this discussion. Our deep experience includes:

Board-level credibility developed over 125 years

KPMG is a respected global network of member firms, providing audit, accounting and professional services, and we are a trusted advisor to large and small companies throughout the world.

Knowledge of emerging issues

In our Global I-4 Forum, also known as the International Information Integrity Institute, we convene leading cyber security professionals from around the world to discuss emerging threats, regulatory challenges and solutions for various industries.

Proven track record and an objective, knowledgeable advisor

Our global network of regulated member firms has an unwavering commitment to precision, quality and objectivity in everything we do.

...to across the enterprise.

Our team can help you deliver on the promise of cyber security to all levels of your enterprise by providing:

Technical security that aligns with your culture

We combine technical proficiency with deep, cross-functional business expertise to create a security culture throughout your respective functions and activities.

An ecosystem approach

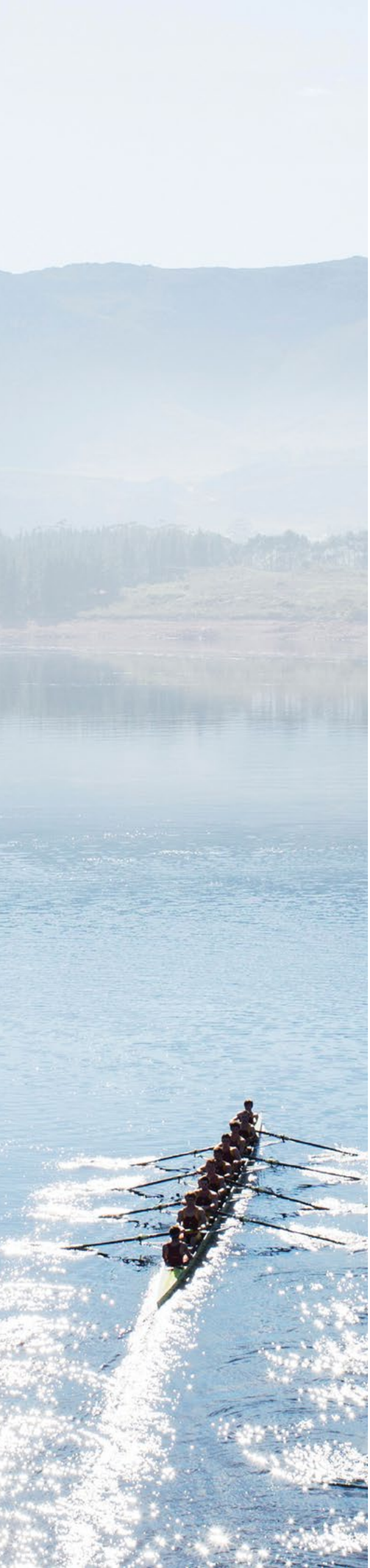
In addition to our own cyber security experience, we're able to leverage expertise from across our cyber security ecosystem. This allows us to tap into knowledge and insight from key alliance partners in areas such as emerging threats, new technologies, competitive intelligence and more.

Enterprise-wide security transformation

Technology is only one part of a transformation. We also help you design processes for employees, customers, suppliers and other stakeholders; prepare your organisation to adopt the new technology; and help change behaviours throughout the enterprise.

Security transformation across different geographies and cultures

KPMG understands cyber security risks, regulatory impacts, change management, forensic investigations and other factors that may change from one country to the next. We have a global network of more than 3,000 cyber security professionals, plus multi-disciplinary collaboration with 155,000 other professionals in KPMG member firms across more than 150 countries.



Case Study: Identity and access management

The challenge:

A major Australian bank needed a new staff identity management system to keep it safe, reduce audit items, and raise the staff user experience. Its internal identity management was maintained by disparate teams, resulting in a manual, and often immature process, to manage the identity lifecycle of internal staff and vendors. This was directly impacting productivity.

The KPMG solution:

KPMG was engaged to integrate the bank's chosen identity management technology, and to make it easier and faster for people to get the right access to the right systems, at the right time. KPMG helped to reduce the time for new user account creation by 95 percent. Staff can be productive from day one; outgoing staff profiles are disabled automatically; and requests can be submitted and tracked via a central interface. The implementation has dramatically reduced fulfilment effort required by lifecycle management staff.

Areas of assistance:

- architectural solution analysis and design
- identity management system deployment and configuration
- training, documentation and knowledge transfer
- testing of the deployed solution.

"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."

Jeremy Knight,
Director, KPMG Australia

Case study: Securing a global retail environment

The challenge:

An Australian owned, global retail fashion provider engaged KPMG to assist in the creation of a cyber security strategy that addressed; current maturity weaknesses, risks to critical assets, and enabled organisation strategy. A chief concern for the organisation was the need for a modern, standard and scalable cyber security strategy that would enable the business's short and long term strategic goals. The organisation was guided by recent global cyber events - particularly those affecting the retail industry, to align its processes to industry better practices.

The KPMG solution:

KPMG's Cyber Security professionals brought the firm's technology experience, cyber security knowledge and insights to work for the company. Working shoulder-to-shoulder with the client, the team began by performing a holistic review of the current cyber security controls across the following six areas: Leadership and Governance, Human Factors, Information Risk Management, Operations and Technology, Resilience and Crisis Management, and Legal and Compliance. The transformation process continued by benchmarking these results against the maturity of the industry to highlight key improvement opportunities. The team helped the business to identify the business critical assets and map their underlying threats. This gave the organisation a view of what needs to be protected and what is critical to operations. This information was then leveraged to provide a tailored cyber security strategy that encompassed key uplift activities prioritised for what is achievable, impactful on reducing risk, and aligned to strategic outcomes.

Areas of assistance:

- review of the current state of cyber security maturity
- identification of specific and industry threats, and
- critical business assets
- elicitation of key activities to uplift cyber security
- creation of a strategy for cyber security.

Case study: Developing a holistic GRC strategy

The challenge:

When a national telecommunications provider centralised its security activities into a Security Operations division, the division was tasked with ensuring the organisation had an adequate cyber risk profile. It needed to adhere to constantly changing regulatory frameworks, as well as to rationalise, coordinate and standardise its teams, processes and outputs.

The KPMG solution:

KPMG was engaged to help, beginning with the implementation of the RSA Archer Risk, Compliance & Findings Management modules for regulatory compliance automation. The team facilitated workshops to define a medium-term strategy and end-state, as well as refining processes using LEAN principles. KPMG configured a number of bespoke modules to assist with processes, including: third party security due diligence, project security compliance, vulnerability management, a customer engagement portal, and detailed administrative and end-user training documentation. The client now has an integrated GRC framework comprising centralised risk, control and incident registers, which provides improved visibility and accountability. The systemisation of regulatory compliance activities has resulted in a 20 percent reduction in effort required, enabling SMEs to focus on higher-value tasks.

Areas of assistance:

- definition of IT GRC strategy and roadmap
- multi-year, multi-discipline GRC platform configuration
- rationalisation of cyber security processes/functions
- LEAN process optimisation.

Case study: Cyber incident response

The challenge:

An organisation suffered a targeted variant of the 'WannaCry' ransonware cyber attack. The impact included the complete shutdown of staff and vendor integration systems, POS equipment and financial systems. The organisation needed immediate analysis, response planning, stakeholder communications, remediation coordination, and post-incident investigation.

The KPMG solution:

The team provided immediate 'on the ground' support for in-house IT, as well as incident analysis to ascertain the nature of the attack, and the extent of its activities. The team assisted with the recovery of lost data, and the coordination of an incident response plan to ensure removal of the malicious application and recovery. They distributed stakeholder communication, and managed the remediation process to return the business to fully operational status. A post-incident investigation included a training session and controls review. By addressing both the incident and the broader security ramifications, KPMG helped the organisation arrive at a vastly improved cyber security position.

Area of assistance:

- rapid cyber incident response services
- forensic technology investigation
- stakeholder communications
- recovery project management.

Seize the cyber security opportunity

New markets, mergers and sales channels open up new revenue opportunities. However, the question is whether your organisation has the confidence and agility to seize them. According to KPMG's 2018 CEO Outlook Survey, 70 percent of Australian CEOs believe that additional security prompts innovation in their products and service lines. Our team can work with you to help you protect your critical business assets so you can embrace new opportunities and build your competitive advantage.

Contact us

Gordon Archibald
National Lead,
Cyber Security Services
T: +61 2 9346 5530
E: garchibald@kpmg.com.au

Katherine Robins
Cloud Security Services Lead
T: +61 3 8663 8550
E: krobins@kpmg.com.au

Stan Gallo
Partner, Forensic
T: +61 7 3233 3209
E: sgallo@kpmg.com.au

Ian Gray
Defence & National Security Lead
T: +61 2 6248 1230
E: igray@kpmg.com.au

Danny Flint
Digital Trust and Identity Lead
T: +61 7 3434 9191
E: dflint@kpmg.com.au

Campbell Logie-Smith
Business Resilience Lead
T: +61 3 9288 5920
E: clogiesmith@kpmg.com.au

Priyank Baveja
Technical and Architecture Lead
T: +61 3 9288 5125
E: pbaveja1@kpmg.com.au

Max Drabik
IT Governance, Risk
and Compliance Lead
T: +61 3 9288 5379
E: mdrabik@kpmg.com.au

Jeremy Dunn
Strategy and Governance Lead
T: +61 2 9346 6342
E: jdunn4@kpmg.com.au

KPMG.com.au

August 2019. 382791848MC.