Organisations are subject to increasing amounts of legislative, corporate and regulatory requirements to show that they are managing and protecting their information appropriately. Simultaneously, the threats from cyber criminals and hacktivists are growing in scale and sophistication. Organisations need to continually evolve their cyber security architecture to respond to the changing digital environment. By working with your team we can help you take a positive approach to managing cyber risk. This can enable you to take control of uncertainty and turn the digital environment into a genuine strategic advantage.

The cyber security landscape and the associated threats is not a new thing – the speed of evolution is what is changing. The focus on cyber security is increasing rapidly due to many high profile and highly disruptive/damaging security breaches threatening financial and physical damage across critical national and corporate infrastructures.

It is also increasingly common for government buyers and large corporates to demand confidence in information management as a qualifier for lucrative contracts or partnerships. With the stakes so high, organisations must decide on their cyber risk appetite and how they will respond. There is a significant responsibility on executives to assure customers, stakeholders and employees that appropriate cyber security architecture is in place. We can work with you giving you the advice and challenge you need to make decisions with confidence.

One major London-listed company with which we have worked estimates that it incurred revenue losses of some £800 million as a result of hostile state cyber attack – not just through intellectual property loss but also from commercial disadvantage in contracted negotiations.

Jonathan Evans, former Director General of the Security Service MI5, 26th June 2012
WHAT'S ON YOUR MIND?
Do I need help assessing whether the mechanisms to manage our risks are mature?
Am I looking to create a stronger security culture within my organisation?
Do I need a better understanding of whether I comply with the varied regulatory requirements?
Am I looking to take greater control, ensuring that my organisation is prepared for the evolving cyber security landscape?
What should I be considering as part of a cyber security strategy?

OUR APPROACH
Working with your team and conducting a combination of interviews, workshops, policy and process reviews and technical testing, KPMG’s CMA team takes a positive view to managing cyber security, and the program rapidly:

• Identifies current gaps in compliance and risk management of information assets;
• Assesses the scale of cyber vulnerabilities;
• Sets out prioritised areas for a management action plan.

The assessment provides the flexibility to assess the level of cyber maturity on a site by site basis or at a company level. It helps to identify best practice within an organisation and provides comparator information against peer groups and competitors.

In turn, allowing businesses to feel free to navigate the cyber security landscape and achieve their business aspirations.

HOW WE HAVE HELPED OTHERS
A FTSE 100 global service provider had suffered an increasing number of security breaches and also had growing concerns about insider threats as a result of either malicious or accidental data loss.

The client needed to better understand its vulnerabilities, to assess its capability to protect information in line with relevant standards and to provide a remediation plan.

KPMG in the UK completed a detailed and holistic review of the organisation’s cyber maturity, working with the client to align the assessment with ongoing transformation programmes, and delivered a highly detailed report outlining areas of vulnerability with clear plans for remediation.

The remediation formed the basis for the client to achieve further funding for a cyber strategy, gave greater assurance to senior leadership and led to greater customer trust.

WE BELIEVE CYBER SECURITY SHOULD BE ABOUT WHAT YOU CAN DO – NOT WHAT YOU CAN'T

WHY KPMG?
INDEPENDENT
KPMG member firms technical strategies and recommendations are based solely on what is fit and appropriate for your business.

COLLABORATIVE
KPMG’s I-4 forum brings together over 50 of the world’s leading organisations to discuss emerging issues and the solutions which work in an ever-increasing threat landscape.

TRUSTED
KPMG member firms have a long list of certifications and permits to work on engagements for the world’s leading organisations.

GLOBAL, LOCAL
KPMG is a global network of independent member firms of over 155,000 professionals in 155 countries. We have over 2,000 security practitioners globally, giving member firms the ability to orchestrate and deliver to consistently high standards worldwide.

AWARD WINNING
KPMG in the UK shines in independent recognition: Our Cyber security team won the Information Security Consultancy award in 2011 and 2012. The team also won the MCA award in 2011 and 2012.

Contact us:
Stephen Bonner
Partner, Cyber Security
T: + 44 (0)78 8790 6509
E: stephen.bonner@kpmg.co.uk

Martin Tyley
Partner, Cyber Security
T: + 44 (0)113 231 3934
E: martin.tyley@kpmg.co.uk

Ruth Anderson
Principal Advisor
T: +44 (0)20 7694 2492
E: ruth.anderson1@kpmg.co.uk

Cyber Maturity Assessments are offered by other KPMG member firms, to speak to your local contact outside the UK, please contact Ruth Anderson for more details.