KPMG

cutting through complexity

FEEL FREE

A NEW APPROACH TO CYBER SECURITY

THE PRINCIPLES OF OUR APPROACH

We believe cyber security should be about what you can do – not what you can't.

DRIVEN BY BUSINESS ASPIRATIONS

We work with you to move your business forward. Positively managing cyber risk not only helps you take control of uncertainty across your business; you can turn it into a genuine strategic advantage.

RAZOR SHARP INSIGHTS

In a fast-moving digital world of constantly evolving threats and opportunities, you need both agility and assurance. Our people are experts in both cyber security and your market, which means we give you leading edge insight, ideas and proven solutions to act with confidence.

SHOULDER TO SHOULDER

We work with you as long term partners, giving you the advice and challenge you need to make decisions with confidence. We understand that this area is often clouded by feelings of doubt and vulnerability so we work hand-in-hand with you to turn that into a real sense of security and opportunity.

FEEL FREE

A positive approach to managing cyber risk can set organisations free

UNDERSTANDING THE CYBER SECURITY LANDSCAPE

The digital environment presents opportunities for businesses that want to seek out new markets and are prepared to invest in transformational change. The last ten years have seen a rapid emergence of new technology, greater connectivity for organisations and individuals, and a 24/7 approach to global commerce. However, this has left many organisations behind the curve and struggling to achieve their business aspirations without feeling exposed to cyber security risk.

Every day we hear of new vulnerabilities, attacks and incidents. A recent report[1] by renowned think-tank *The Centre for Strategic and International Studies* quoted losses of $375 – $575 billion, and suggests that cyber crime might extract up to 20% of the global economic value created by the internet through fraud and espionage.

The constantly evolving threat landscape means that cyber risk is an everyday business consideration. This undoubtedly presents a feeling of vulnerability, which has been leveraged by some to increase budget and to sell products. We have often found that this results in significant sums of investment on ineffective programmes with poor alignment to risk and business imperatives. Cyber security is not a quick technical fix nor is it a matter solely for the IT department.

At KPMG we see all too often that these behaviours leave leadership wondering what they really need to do, how much is really enough and who they can trust to help them get it right.

We believe that by turning traditional thinking on its head, adopting a positive approach to managing cyber risk, will set organisations free to achieve their business aspirations.

[1] Net Losses: Estimating the Global Cost of Cybercrime, June 2014

FREE FROM FEAR

Scaremongering is an easy tactic, but staying on top of the evolving threat landscape and how it impacts you can remove fear, uncertainty and doubt.

Understanding the external threats from hacktivists, organised criminals, industrial espionage and increasingly National States is important. However, it is all too easy to ignore the insider threats posed by careless, disgruntled or malicious employees. Attackers are frequently gaining access to employee's accounts through phishing emails and other socially engineered attacks. Bribery and intimidation is also still commonplace in most parts of the world. By managing the external and internal threats together, rather than separately, creates an integrated approach that removes the fear and uncertainty of attack sources.

Many attackers are simply using different means to achieve a very old objective; be that theft, subversion, sabotage or espionage. Drawing parallels between security in the real and virtual worlds can remove fear of the unknown.

At KPMG we assess the motivation and intent of the attacker in both the real and virtual worlds to see how they might compromise your systems. Based on this insight, we can then challenge and advise you on how to position your defences.

Building in agility, with the expectation of change and disruption, enables you to architect an environment that is secure by design.

LEVERAGING INDEPENDENT AND TAILORED ADVICE CAN GIVE YOU THE CONFIDENCE TO PURSUE YOUR GROWTH AMBITIONS

Putting the correct foundations in place around governance, risk and compliance is the place to start. You can then achieve a balance of technical security, internal capability and the appropriate usage of technology and outsourced services.

We believe that successful organisations are ones that integrate cyber risk management into all their activities. Those that practice sound transformational principles rather than succumbing to knee-jerk reactive solutions can create a comprehensive approach that focuses on what they can do – not what they can't.

FREE TO CHALLENGE

The UK government is regularly implementing initiatives to boost awareness of cyber threats. Boards need to challenge their teams to gain answers to the right questions before they themselves are challenged by stakeholders on their capability and control. Being able to identify, prioritise and protect the information lifecycle helps you to move confidently, safely and securely.

At KPMG we can help you understand your dependencies on your supply chain, work with your community to understand cyber risks, share information on threats and improve readiness to respond together.

Having a robust strategy and architecture in place will enable you to access clear and actionable management information to give you strength in your decision making; provide access to timely threat insights; trusted information-sharing networks; and credible benchmarks against peers and competitors. Information sources need to be impartial and independent of specific vendor agendas. Accessing sources you can trust allows you to test and examine the right mix of technology, service providers and internal capability to create a blend of control and visibility.

We believe that this is where collaboration and knowledge will differentiate to deliver business advantage. By leveraging collective experience of those you trust, you will have confidence to execute new ideas, approaches and solutions to respond to today and tomorrow's security issues.

FEEL FREE TO SPREAD YOUR WINGS

FREE TO INVEST

With each aspect of emerging technology, new considerations arise; from the adoption of cloud technologies, the proliferation of social media, to remote working. These are all potential high growth investment options when managed effectively.

Similarly, the rise of mobile technology and its applications is relevant to all sectors and business models. Organisations need to make choices around these new technologies, understand the cyber security issues up front, to strike the right balance between risk and opportunity.

At KPMG we can work alongside you to identify how much investment is appropriate to ensure that cyber risk management is an enabler to achieve your business aspirations.

Leveraging independent and tailored advice on which security services, technologies and approaches fit your culture, can give you the confidence to pursue your growth ambitions. We can help you develop a broad understanding of the threat environment which is specific to you, the regulatory landscape in which you do business, and your own asset environment.

We believe that investing in a proactive approach to cyber risk management delivers wider commercial benefits. It is about having the confidence that as your business increasingly moves into the digital world, it is able to grow in an informed and agile manner.

CYBER RISK MANAGEMENT IS AN ENABLER

FREE TO CHANGE

Currently many firms only act if and when a serious breach or failure occurs. Taking a proactive security stance can slow the attacker's progress and identify their actions early. Developing an adaptive approach can prevent downtime, avoid expensive disruptive responses to incidents, and maintain business operations. Thinking through the cyber attack scenarios and the changing threat landscape will help you understand how your business might be targeted and how to configure your defences.

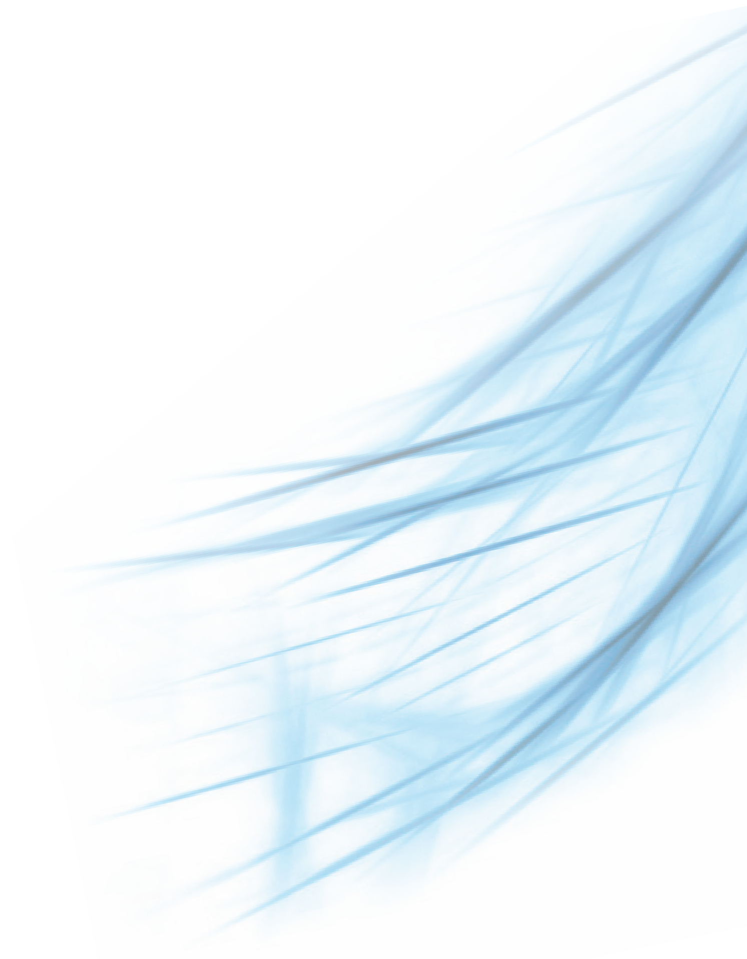
At KPMG we focus our approach on making best use of an organisation's scarce resources. We start at the beginning with a concept of secure by design, where money is invested early in the development lifecycle to achieve greater impact.

By focusing on building solid foundations, you can underpin your security operations with leadership, sponsorship and governance. This helps set the conditions for the right culture where everyone recognises that security is the responsibility of all, and each individual understands the part that they can and must play.

Having the confidence to transform in this way integrates strategy, policy, governance, organisation, process, skills and technology.

We believe that businesses who accept cyber attacks as an inevitable part of today's business landscape and who build in proactive safeguards and responses, will secure the future of their business.

SECURITY IS THE RESPONSIBILITY OF ALL



WE ARE...

AWARD WINNING

Whether it's SC Magazine or the MCA Awards, KPMG shines in independent recognition. Forrester also recognises KPMG as a leader in Information Security Consulting, highlighting our strong focus and ability to take on challenging engagements.

INDEPENDENT

We are not tied to any technology or software vendor. All of our recommendations and technical strategies are based solely on what is fit and appropriate for your business.

GLOBAL, LOCAL

We have over 2,000 security practitioners working in KPMG's network of firms, giving us the ability to orchestrate and deliver to consistently high standards globally. KPMG member firms can service your local needs from information security strategy and change programmes, to technical assessments, forensic investigations, incident response, training, and even ISO 27001 certification.

COLLABORATIVE

We facilitate and work with collaborative forums to bring together the best minds in the industry to collectively solve shared challenges. KPMG's I-4 forum brings together over 50 of the world's biggest organisations to discuss emerging issues and solutions.

TRUSTED

We have a long list of certifications and permits to work on engagements for the world's leading organisations.

THE DIGITAL ENVIRONMENT PRESENTS MANY OPPORTUNITIES FOR BUSINESSES THAT WANT TO SEEK OUT NEW MARKETS AND ARE PREPARED TO INVEST IN TRANSFORMATIONAL CHANGE

CONTACT US

Gerben Schreurs
Partner, Forensic
T: +41 58 249 48 29
E: gschreurs1@kpmg.com

Jean Paul Ballerini
Senior Manager, Cyber Security
T: +41 58 249 55 64
E: jballerini@kpmg.com

Matthias Bossardt
Partner, Cyber Security
T: +41 58 249 36 98
E: mbossardt@kpmg.com

Roman Haltinner
Senior Manager, Information Protection and Business Resilience
T: +41 58 249 42 56
E: rhaltinner@kpmg.com

kpmg.ch

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor 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.