KPMG

Securing the future of financial services

Driving innovation with confidence – a global discussion paper

Insights from a round-table discussion between
*KPMG cyber security practice leaders.

Navigating the evolving cyber security landscape

Actively managing customer trust in the financial services sector, amidst constant and accelerating technological disruption, presents leaders with fresh challenges and new revenue opportunities. Trust has become central to customer experience, and financial services organizations are demonstrating a commitment to trust through their cyber agenda.

Our discussion with a group of country cyber security practice leaders touched on a number of the key questions which are currently being considered by security leaders in financial services.

For instance, the growth of virtual banks is not just a competitive threat to incumbents; it's also forcing the pace in IT infrastructure transformation in order to keep pace with new players.

AI and bots may be revolutionizing interactions and transactions, but these must also be kept on a leash, to ensure they are secure and trustworthy, and that they contribute to rather than disrupt the customer experience.

With everything available as-a-service, financial services organizations must ensure their governance and controls are sufficient to cope with a growing range of partners, particularly when it comes to supplier selection, data security and privacy.

And the roles of risk officers are set to change as cyber policy, risk and compliance moves from the Chief Information Security Officer (CISO) to the Head of Cyber Risk, opening the door for a convergence of fraud and cyber risk.

It's an exciting time to be involved in cyber security in financial services, and we hope the insights in this discussion paper help to further the debate and, more importantly, stimulate innovation in risk management.

Charlie Jacco

Global Financial Services Lead, Cyber Security, KPMG International and Partner.

KPMG in the US

The impact of virtual banks

Speed of change, supplier ecosystems, regulatory fragmentation and customer experience.

Akhilesh Tuteja
Global Cyber Security practice Co-leader, KPMG International and Partner, KPMG in India

Henry Shek
Head of Cyber Security, KPMG in China

The need for speed is a major issue. Financial services organizations are competing not only with their traditional peers, but also with an increasing number of agile, digital disruptors such as virtual banks. The pace at which these new players are developing is forcing traditional banks to adopt more agile approaches to managing their own IT infrastructure. A major transformational change of a bank's platform used to take anything between 2 and 5 years. But now they're up against players with no legacy systems to upgrade and they are forcing the pace. Suddenly people are talking about upgrading banking systems every 4-6 months. That places huge pressure on a bank's IT people – who have to manage the security implications of accelerating change while simultaneously dealing with the legacy of elderly systems and sunk investment.

Virtual banks introduce deeper co-dependencies. Digital disruptors typically have no physical branches and in some cases no ATMs either – which means that they rely wholly on an electronic, cloud-enabled ecosystem, with non-traditional partners providing touch points to reach customers. These virtual players will be working closely with vendors and suppliers, including, for instance, convenience stores to provide cash outlets. Having significantly less infrastructure than their more established peers greatly accelerates their speed to the customer. But it also adds increasing complexity to cyber risk management, which is still in its relative infancy.

China is well on its way to being cashless with digital wallet adoption penetrating into all sectors and customers on mobile.[1] A large proportion of cashless payments use QR code – 'quick response' codes – which can be read by a camera or smartphone for payment. Digital payment providers are already commonplace in China and customers are the driving force for these digital adoptions. Retail and commercial businesses in particular are adapting quickly to ensure they remain relevant to the needs of their customers and are enabling their digital agenda.

Risk management and cyber security remains a challenge. In the rush to provide a superior customer experience, financial services organizations are embracing robotics, AI blockchain and real-time data analytics. On top of this we have the new Faster Payment System and Open Application Programming Interface, ushering in a new spirit of competition between banks and non-bank players. And with AI and biometrics used for customer identification and management (including customer e-onboarding via remote account opening), financial services organizations have to keep a close eye on fraud and be aware of ever-changing fraud scenarios. Cyber criminals are already using new and advanced methods to manipulate security weaknesses and traditional security and protection mechanisms may not be sufficient to deal with AI and advanced technology-enabled attacks. We expect to see more financial services organizations embed cyber security into their digital and business strategy, investing in cyber security as part of the innovation budget, creating a holistic process to become more resilient to evolving cyber threats. Indeed, cyber security will likely become part of every digital adoption.

[1] https://www.straitstimes.com/asia/east-asia/chinas-march-to-be-the-worlds-first-cashless-society-china-daily-contributor, 2019.

Kunal Pande
Head of Cyber Security,
Financial Services,
KPMG in India

A more proportionate regulatory environment can help reduce barriers to entry for virtual banks. We're seeing the emergence of sandboxes across the globe. These are managed programs lasting several months that allow early-stage fintech start-ups to test their offerings in a limited market environment, under regulatory supervision, but without having to be fully licensed. This will enable financial services organizations to experiment with a variety of new solutions. However, as they 'graduate' from the sandbox program they will need to increase the security embedded in their offering and ensure it is both robust enough and secure enough to scale.

Paul Taylor
Head of Cyber Security,
Financial Services,
KPMG in the UK

The battle for consumer financial services is heating up with the advent of open banking under PSD2 (and other similar legislation globally) creating an environment where new entrants can concentrate on the 'front of house' in banking – basically positioning themselves as account aggregators and payment initiators. These entrants can focus on offering holistic financial services to their customers, building digital trust and stickiness, with traditional banks increasingly seen as banking-as-a-service utility providers. Such a change raises many questions over the security and regulation of these new entrants; it also brings added complexity, as financial services organizations must implement effective fraud controls when they do not directly control the digital interactions with customers.

The rise of AI and bots

Maintaining security and keeping bots on their leash

Akhilesh Tuteja

Cognitive automation is taking off in a big way across the global financial services sector, powered by new-age AI technology. But how do you make AIs secure when classic programming technology controls are no longer applicable and the logic behind the AI is becoming increasingly complex and inscrutable? On the back-office side, we're seeing clients deploy robotics in some shape or form. And robotics to me is like spreadsheets on steroids! If you found managing compliance around spreadsheets difficult, imagine what it's like with robotics!

Henry Shek

Chat bots are fairly common and are being implemented across many Chinese financial services organizations. Most of them are designed to facilitate the customer journey, with 'question-and-answer' type algorithms. When the bots start making banking decisions, accountability becomes an issue. The process for letting bots run, and the 'fail-safe' that leads to human intervention (e.g. from call centers) must be seamless, to avoid a frustrating customer experience. In general, many financial services organizations have some way to go before they're able to achieve a sound balance between the robot and the physical.

Kunal Pande

Straight-through processing is another phenomenon, as the financial services sector focuses on automation. By allowing end-to-end digitization and automation, straight-through processing speeds up transaction time and makes the entire payment process more streamlined and free from human intervention. High speed lack of human intervention brings benefits and risks.

Paul Taylor

Trust and fairness will almost certainly become key concepts for the AIs of the future. As financial services organizations look to harness machine learning and conversational bots, it will be crucial that they embed security and privacy from day 1 - not just in the design, but in the way they train and operate AIs. Financial services organizations will need to demonstrate AI integrity and robustness, but also meet regulatory and customer expectations. The decisions made by AIs are likely to face rising pressure to be free from prejudice, explainable and open to challenge. Organizations should ask themselves whether they are sufficiently creative about their governance of AI operations: should they treat them less as software and more as a person in future – applying many of the principles of identity and access management, behavioral monitoring and even insider threat detection?

Managing complex third-party relationships

The explosion in open banking models, cloud and managed service providers is placing strain on traditional control and compliance functions.

Akhilesh Tuteja

Shadow IT is going through the roof. Central organizations are wondering how to retain control when their various businesses are able to buy and deploy technology without undergoing strict internal governance processes. On top of this, we have the compliance implications of using third parties. Regulators around the world are becoming more and more ruthless and demanding in their expectations of how financial services organizations manage third parties. They expect the same degree of control a financial services organizations would have over its own operations and third parties themselves to demonstrate similar levels of control consciousness. All of the US regulators are issuing recommendations or notices to big financial services organizations in the US on third party risk.

Henry Shek

As fintech and technology players become part of our ecosystem, financial services organizations must stay on top of collaboration in order to maintain an acceptable level of risk. This means ensuring that the application programming interfaces at the heart of supplier ecosystem interactions are secure, and that sensitive data is being handled appropriately. We're still pondering how to manage these whole, third-party ecosystems involving cyber, outsourcing, cloud, mobile and customer data, all of which are top of the technology risk agenda.

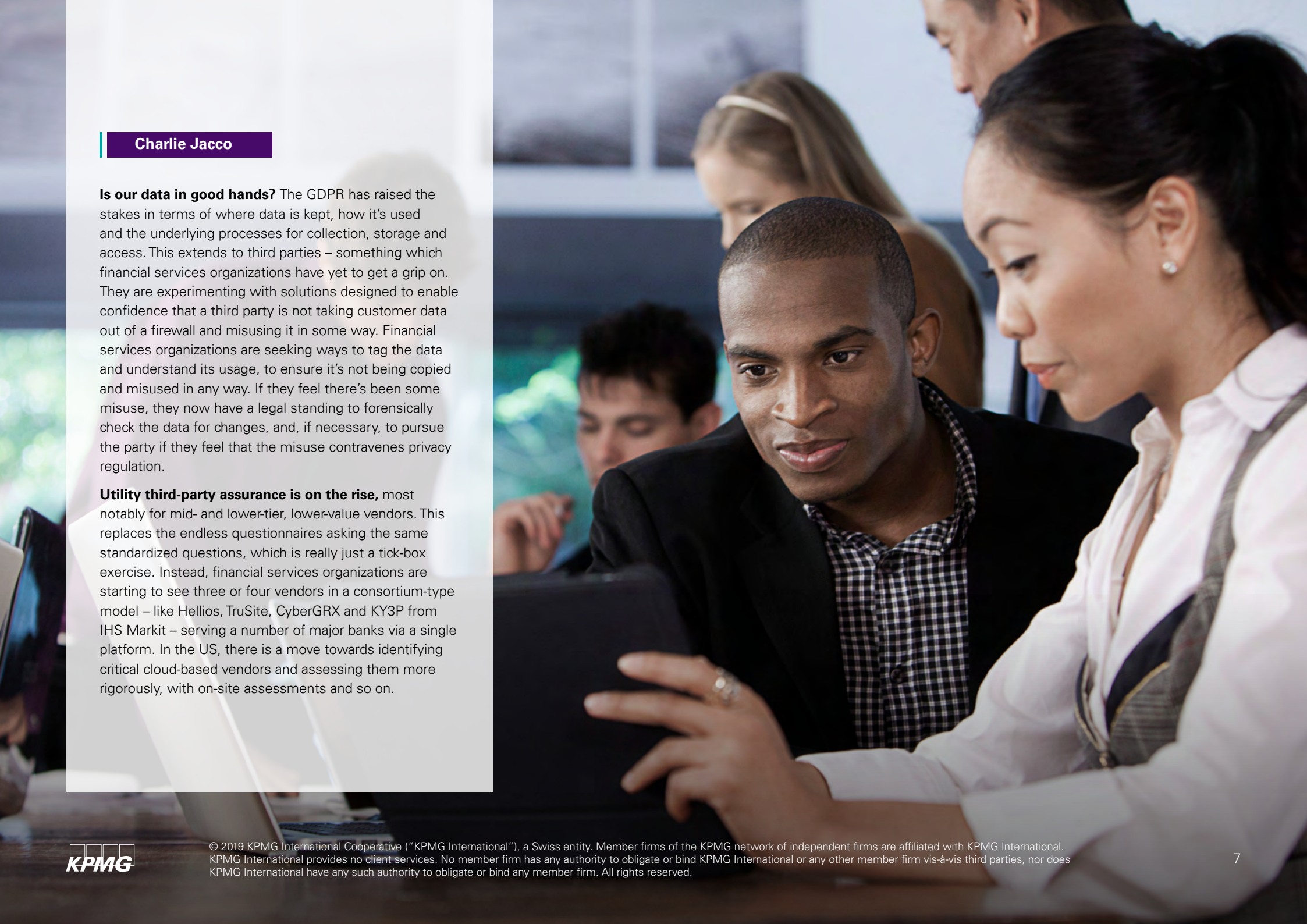
Kunal Pande

Payment banks have emerged in India in the last couple of years, offering only payment products, which has led to a lot of e-commerce platform integrations. On the payment side, there have been many new open payment products such as the Unified Payment Interface (UPI) which allows bank customers, both consumers and businesses, to use even third-party providers to manage their payment requirements. This shift has created a completely new ecosystem where banks and non-banks are competing with each other. The regulator is looking at this area very carefully, especially given the cyber security crimes targeting payment systems.[2]

Third party relationships are proliferating as financial services organizations in India work with various partners – some of whom become very integrated into the overall value delivery. This is attracting a lot of attention from the regulator, because many of these partners are not licensed, regulated entities.[3] Therefore, the onus is on the organizations to demonstrate that they're carrying out a proper risk assessment and putting in appropriate cyber security controls.

[2] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF, 2016.

[3] https://rbidocs.rbi.org.in/rdocs/notification/PDFs/NT41893F697BC1D57443BB76AFC7AB56272EB.PDF, 2016.



Charlie Jacco

Is our data in good hands? The GDPR has raised the stakes in terms of where data is kept, how it's used and the underlying processes for collection, storage and access. This extends to third parties – something which financial services organizations have yet to get a grip on. They are experimenting with solutions designed to enable confidence that a third party is not taking customer data out of a firewall and misusing it in some way. Financial services organizations are seeking ways to tag the data and understand its usage, to ensure it's not being copied and misused in any way. If they feel there's been some misuse, they now have a legal standing to forensically check the data for changes, and, if necessary, to pursue the party if they feel that the misuse contravenes privacy regulation.

Utility third-party assurance is on the rise, most notably for mid- and lower-tier, lower-value vendors. This replaces the endless questionnaires asking the same standardized questions, which is really just a tick-box exercise. Instead, financial services organizations are starting to see three or four vendors in a consortium-type model – like Hellios, TruSite, CyberGRX and KY3P from IHS Markit – serving a number of major banks via a single platform. In the US, there is a move towards identifying critical cloud-based vendors and assessing them more rigorously, with on-site assessments and so on.

Rethinking risk management

The evolution of first- and second-line risk and changing roles of risk officers.

Charlie Jacco

The traditional CISO role is breaking up. Regulators have viewed this primarily as a level 1.5 defense mode, with the CISO owning risk policy all the way through to control and implementation. But simply telling the Board how many vulnerabilities were discovered last month does not really give a full picture of cyber risk. In the US, the Office of the Comptroller of the Currency (OCC) and the Fed are telling big financial services organizations that first-line risk should move to a new role of Head of Cyber Risk. Given that they're reporting either to the Risk Committee or to the Head of Operational Risk, regulators really want cyber risk to be part of the operational risk framework, with separate reporting.[4]

The ultimate goal is to have someone in the risk organization creating policy and risk appetite statements and lines of business objectives, and having the business approve them. So, we're seeing a challenger to the CISO role. And consequently, other traditional first-line portions are moving to second line, like fraud risk and fraud operations, leading to a convergence of fraud and cyber risk. You're starting to see fraud data, anti-money laundering (AML) data, cyber security operations data, and threat-hunting data all fused together in one place as second-line risks.

Kunal Pande

Where does fraud risk fit in? This begs two questions: what does the organizational model look like and how is it being governed? Some organizations have decided to centralize fraud risk and fraud operations, with fraud risk as second line and fraud operations as first line. But then they realize the way they view fraud differs between B2B payments and private wealth, or between credit and retail. So maybe we need more of a hub-and-spoke, federated model incorporating payback-chargeback. In this way, when something fraudulent is discovered, it can be charged back to the relevant business. However, you also need to retain a centralized view over challenges such as bots, which can take over accounts by penetrating the firewall and manipulating data. These kind of anomalies can spread quickly, so it's vital to have a bigger picture of their wider risk.

Akhilesh Tuteja

There's a swing towards machine learning to let the bots figure out fraud scenarios; currently they're not smart enough and are missing a lot. The bots can't tie different fraud instances together, as the fraudsters are purposely coming in below a certain threshold and trying alternative approaches like account takeovers. In response, large financial services organizations are starting to deploy machine learning to identify patterns of fraud behavior and spot signs of fraud.

[4] https://home.kpmg/xx/en/home/insights/2018/07/operational-resilience-fs.html, KPMG in the UK, 2018.

Charlie Jacco

Paper is on the way out. In the US at least, the rising volume of data, and the subsequent analysis, makes paper-based Risk Control Self-Assessment (RCSA) and metrics reporting too expensive and onerous. And with regulators, external and internal auditors all asking about the effectiveness of controls, you spend too much time and energy collecting and reporting evidence, which distracts you from more important, strategic work. So, there's a move towards automated monitoring of key controls on a more current basis, so that everyone can view it in real time.

Paul Taylor

Are we moving towards real time supervision? It's apparent that automated monitoring of controls compliance can help financial services organizations meet regulatory reporting requirements. I wonder how long it will be before we see regulators looking for direct feeds of cyber controls information from the organizations they supervise? All the while, those same regulators will likely be investing in supervisory technology (SupTech) to undertake their own risk analysis and challenge financial services organizations' views of their security. The FCA in the UK has already undertaken a pilot of digital regulatory reporting.[5] It's very early days, but the direction of travel is clear. I think that we will see a very different line of defense (LoD) model for the future, with regulators playing an increasingly vocal role.

[5] https://www.fca.org.uk/digital-regulatory-reporting, 2019.

KPMG can help you turn cyber risk into opportunity

The global network of business-savvy cyber security professionals at KPMG understand that businesses cannot be held back by cyber risk. Our professionals recognize that cyber security is about risk management – not risk elimination.

No matter where you are on the cyber security journey, KPMG can help you reach the destination: a place of confidence that you can operate without crippling disruption from a cyber security event. Working shoulder-to-shoulder with you, we can help you work through strategy and governance, organizational transformation, cyber defense and cyber response. And KPMG doesn't just recommend solutions — they also help implement them. From penetration testing and privacy strategy to access management and cultural change, we can help you every step of the way.

Contact us

Akhilesh Tuteja

Global Cyber Security practice Co-leader, KPMG International and Partner,

KPMG in India

E: atuteja@kpmg.com

Charlie Jacco

Global Financial Services Lead, Cyber Security, KPMG International and Partner

KPMG in the US

E: cjacco@kpmg.com

Henry Shek

Head of Cyber Security

KPMG in China

E: henry.shek@kpmg.com

Kunal Pande

Head of Cyber Security, Financial Services

KPMG in India

E: kpande@kpmg.com

Paul Taylor

Head of Cyber Security, Financial Services

KPMG in the UK

E: paul.taylor@KPMG.co.uk

kpmg.com/socialmedia

Designed at: KGS
Publication date: August 2019