KPMG

DYNAMIC CISO

Digital risk: A new security frontier

March 2019

KPMG.com/in

Table of contents

Foreword: Grey Head Media

Navigating risk in the evolving business and technology landscape is perhaps the most important topic for any boardroom today. In this age, where technology is business or vice-versa, risk forecasting and management are key to an organisation's future and growth.

As the business landscape transforms further due to the application of digital technologies, adoption of extreme automation, rising API economy and growing hyper-localisation, preparing for the next major corporate rig will be more challenging and very hard to predict.

Because the technology changes are faster than the pace of their adoption in the real world, the landscape of business risks is constantly shifting. Both CISOs and the business stakeholders have a responsibility to address these emerging problems. Simultaneously, there's also a need for high-level preparedness to address and mitigate the risks that crop up from factors such as intense competition, ever-changing regulatory/legislative landscape etc.

While the digital tsunami is and will always remain an irreversible trend in the unforeseeable future, it is also critical to be mindful and risk-aware of the growing attack surface that has been created for the threat actors to exploit.

Further, a lot of risks that have emerged in the recent past, are uninsurable risks and also very unpredictable. Risks emanating from a supply chain disruption, abrupt regulatory changes, and a sudden situation created by Merger/Acquisition are mostly not known in advance. While these risks are to be dealt at a group level, technology has a make or break role to play from a data integrity and data security point of view.

Neither the business nor the technology leaders can afford to be ignorant and overconfident about the emerging landscape of business and cyber risks. And therefore, it is imminent to be prepared to navigate businesses through the challenges of the digital world.

Rahul Neel Mani
Co-founder and Editor
Grey Head Media

Foreword: KPMG in India

Digital technologies have become fundamental to operate in today's environment and businesses have seen tremendous shift in operations with digital technologies being embraced and the power of data being leveraged. CEOs and boards are taking personal ownership of driving digital adoption across enterprises and enabling enterprises to be ready to operate in this new environment.

On one side, digital transformation is bringing thorough agility and ability to convert disrupting forces into opportunity and at the same time it brings forth a unique aspect of building **'digital trust'** for complete acceptance by all stakeholders. Customers and regulators are increasingly demanding for increased transparency and visibility to ensure right balance is built.

With the rapid adoption of digital technologies, management across enterprises are evaluating the adequacy of existing risk management practices and also reconsidering the frameworks being adopted for managing risks.

Traditional approach is not designed to deal with the inherent characteristics of digital era, which includes rapid pace of technology change, agile operating model and limited availability of skill sets.

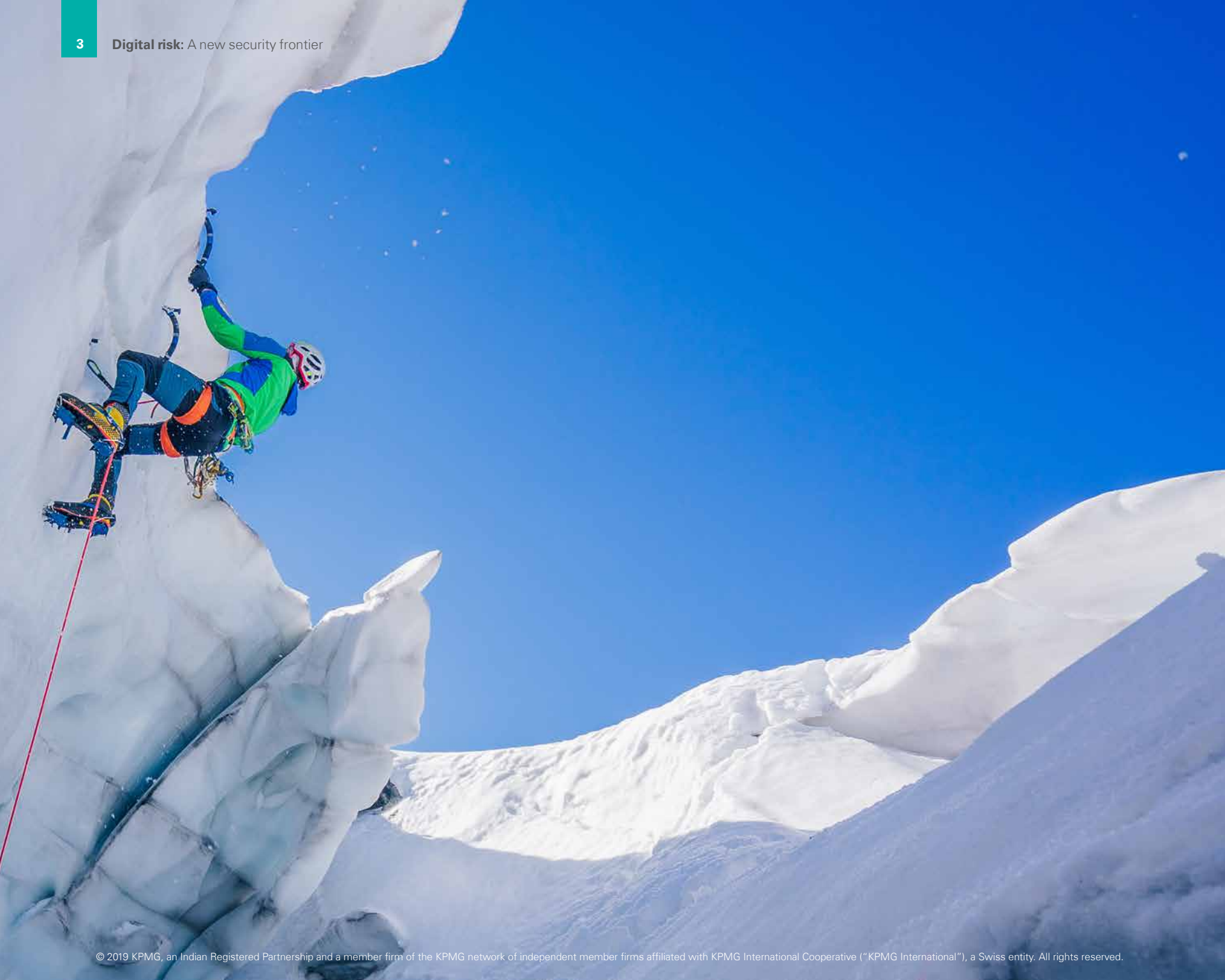
This report talks about emerging perspectives on the dynamic nature of risks to which enterprises are subjected and has been structured to provide a view on the following key domains:

- Digital risk and imperatives
- Risk management frameworks
- Defence mechanism and compliance measures

The report also includes industry survey findings which facilitates in providing a view from industry leaders. This report also focuses on key strategic aspects such as prioritisation of digital risks, dedicated focus to manage digital risks, budgeting, implementation aspects such as reskilling workforce, redeveloping frameworks, etc.

We hope you find the report insightful.

Atul Gupta
Partner and Head,
IT Advisory, Cyber security - Leader



Executive summary

Digital transformation is integration of digital technology into all areas of a business, resulting in fundamental changes to businesses operations and how businesses deliver value to its customers. In this digital transformation journey, businesses have realised the impact that digital media holds on their operations. It has already transformed industries such as media, transportation, and retail and is now sweeping through financial institutions. However, when it comes to a financial institution's risk function, unique challenges and opportunities accompany digitisation, making global Chief Executive Officers (CEOs) and Chief Risk Officers (CROs) wonder how intensely they can automate critical processes and rely on automated decisions.

There is a rising sense of `cyber certainty' among CEOs, as they recognise that the likelihood of their organisation becoming a victim of a cyberattack is a case of `when,' and not `if'.

From our survey, we have numerous questions on the impact of digitisation on the risk function's mandate, role, and organisation (including the several lines of defence); the capabilities, skills, culture, and ways of working required to deliver a digitized risk function.

Business strategy focusing on digital transformation will need to account digital risk as a key aspect into its risk management. Digital risk management is complicated and complex. Several attempts are required in the digital field, in order to deal with real time monitoring, advanced skills and expertise related to IT, and strategic information structure to operation, development, information system, and data integration. Digital risk management is considered to be the next evolution in enterprise risk and security for digital businesses.

67 per cent organisations are already considering digital risk as a key risk in their digital transformation journey.

Today the top three digital risks that organisations have identified are:

1. Operational risks

2. Lack of skillset

3. Vulnerable systems

Most impacted departments by digital transformation:

1. Operations

2. Customer Relationship Management

3. Sales and Marketing

As organisations and individuals within them are at different levels of maturity in terms of their understanding and management of digital risks, a focused effort is required with specialised knowledge, skillset and commitment for managing digital risks on a day to day basis.

Digital technologies are rapidly changing the way that companies create and deliver value to their customers. Over the past five years, digital disruptors have destroyed some businesses and this pace of disruption is accelerating. The digital space is a multi-device, multi-mode, omni-channel world where quality is measured not by schedules, budgets, and defects but by user experience including both external customers as well as employees. A 'one size fits all' strategy is no longer an option.

Also, data breaches and the resultant costs have increased exponentially over the last few years. The adoption of digital technologies is changing the risk landscape.

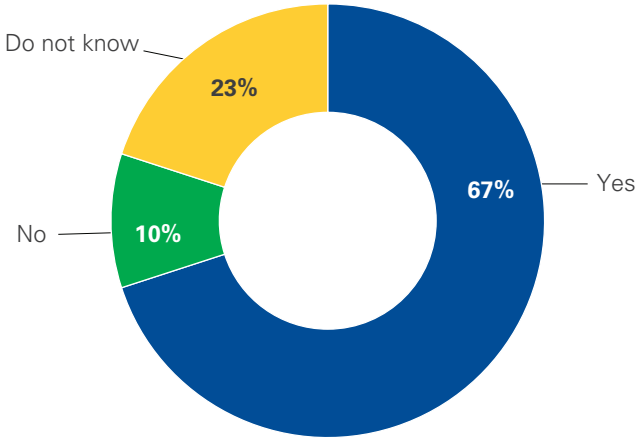
Business strategy focusing on digital transformation will need to account digital risk as a key risk. Several attempts are required in the digital field, in order to deal with real time monitoring, advanced skills and expertise related to IT, and strategic information structure to operation, development, information system, and data integration.

1 Digital risk: A new normal

Digital risk: Key risk

67%

of respondents consider digital risk as a key risk



In today's word while a majority of organisations have clarity when considering digital risk as a key risk in the digital transformation journey, still 23 per cent organisations lack this clarity.

With the intent of digital transformation, organisations are constantly facing increased pressure to have a more systematic approach to deal with digital risk.

- Organisations are expanding their business operations and establishing third party networks which are dynamic, complex and highly integrated across the digital value chain.
- With the highly connected business ecosystem, threats and their impact gets amplified exponentially and mandates continuous monitoring and safeguards.
- Data breaches and the resultant costs have increased exponentially over the last few years. The digital risk landscape is radically evolving. The volume and velocity of data available on digital media is on an exponential growth curve.

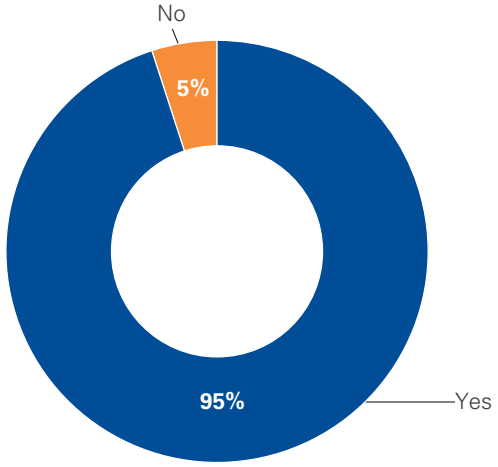
Hence, an organisation needs to have clarity in handling and managing digital risks. This can enable organisations to allocate the required resources.

Understanding overall technology transformation and overall risk setting is all part of forming a culture of confidence within the organisation. The entire organisation needs to apprehend the technology, how the models operate, why certain operational decisions are made by the automated tools and where the explicit risks and opportunities lie.

Digital risk: Chief Digital/Transformation Officer's key responsibility

95%

Of respondents suggests Chief Digital/ Transformation officer to play key roles in managing Digital Risks



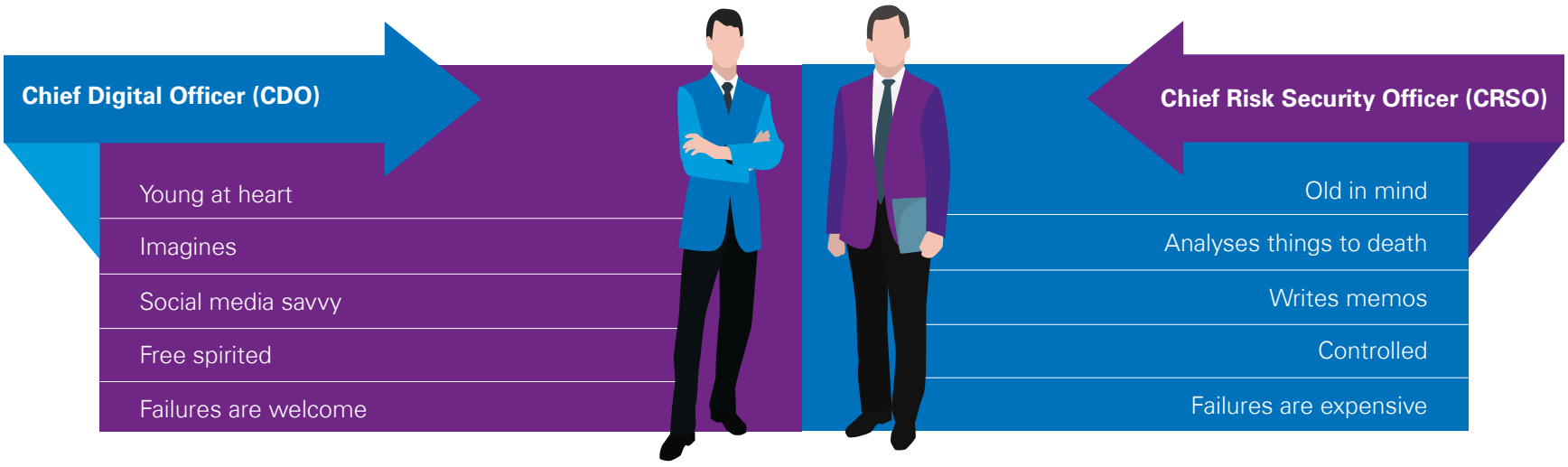
95 per cent of respondents think that digital risk should be considered to be a key responsibility for a dedicated person, such as the chief digital officer or the chief transformation officer, heading the digital transformation of the organisation

As companies integrate digital technologies into key business processes, they will accrue benefits like agility, competitiveness, reaction time and reach. This will also expose thems to greater security threats related to digital business innovation. These threats will require a more sophisticated response and a greatly expanded portfolio beyond traditional risk and security roles today[1].

1. The Rise Of The Digital Risk Officer, Gartner, May 2015

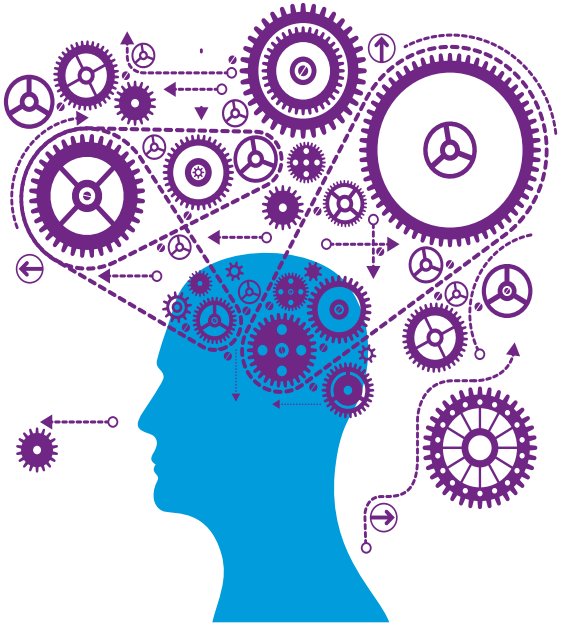
Changing role of Chief Digital Officer (CDO) to Chief Digital Risk Officer (CDRO)

A Chief Digital Officer (CDO) and/or Chief Digital Risk Officer (CDRO) that can design and execute a consistent, unified approach can deliver greater risk assurance for business processes than the fragmented approach which is currently in place at many companies. CDROs are to influence gov-ernance, oversight and decision-making related to digital business. Business structures will need to be re-engineered with security priorities in mind, and will require an executive who is skilled in risk assessment, monitoring, analysis and control. The CDRO will inspire balance between the need to protect the organisation and the need to run the business.



> This is a fact that growth in digital risk specialists has not kept pace with the growth of digital transformation and thus there is an obvious gap. 'Mean time to Hire' for such risks from the market is at all time 'high'. There is a scarcity of 'readymade' skills in this space. The best bet in this scenario is reskilling, upskilling the existing cyber security/IT risk professionals. This may need some time but that is the only solution.

Durga Prasad Dube
Senior VP and CISO
Reliance Industries Limited



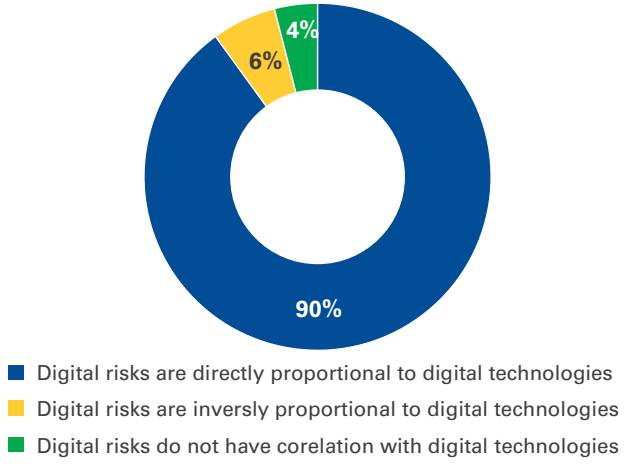
Digital risk: Proportional to uptake of digital technologies

Taking into account the view point from an end user's perspective, a large number of our survey respondents uniformly believe that digital risks are also exponentially expanding to a great extent in proportion to the uptake of digital technologies. Very few of our survey respondents are of the view that digital risks are inversely proportional or have close to zero correlation with digital technologies.

90%

Of respondents believe that digital risk exposure is directly proportional to use of digital technologies

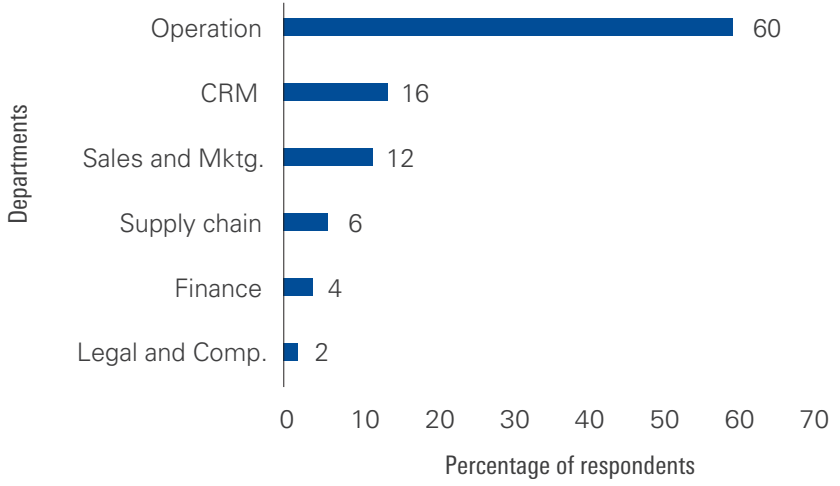
- Adoption of the digital technologies brings greater analytical capabilities for the organisations to give better understanding of their consumer behavior and improvising their services accordingly, however, it also introduces associated digital risks with these technologies, affecting the digital trust of the end customer.
- The ease in usage of digital platforms, the reliability of fulfilment and ability to effectively manage data processing are important factors that have demonstrated positive influence on consumer behavior, nevertheless, consumer's awareness around amount of personal information collected by organisations and their sensitivity towards sharing personal data on digital platforms has indicated the greater need of managing digital risks by the organisations.



> With pervasive adoption of digital transformation in every part of business, digital risks are an inherent part of our lives. Trust and ethics are the two important aspects of it. They have to be built, nurtured and followed. Most importantly, how do you provide assurance to people from whom you have collected the data, is going to be the most critical part.
>
> **Sridhar Govardhan**
> CISO, Wipro Ltd

Enhanced value delivery through digital transformation

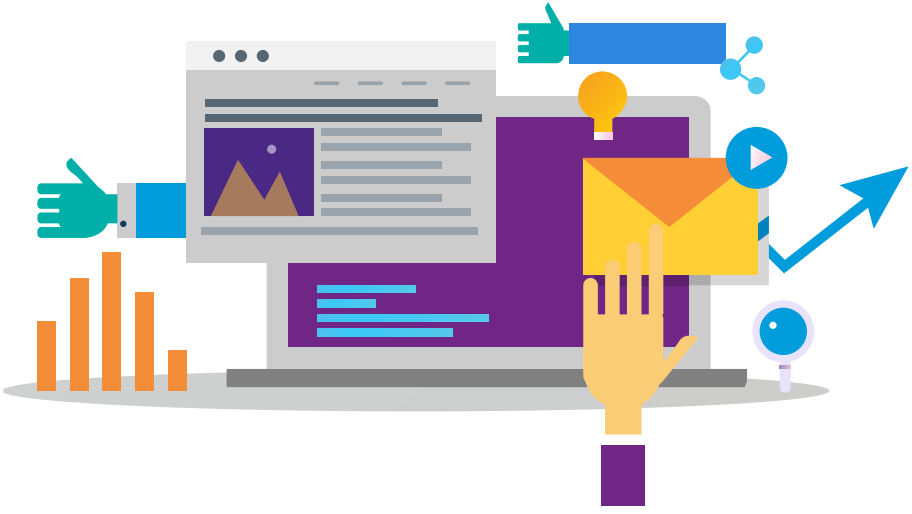
With the increase in use of automation, the aim has been to utilise employees' time for more valuable tasks while the mundane tasks can be automated. Nearly 60 per cent of the survey respondents contemplate that operations will have more value delivered through a digital-transformation programme, followed by 26 per cent of the survey respondents contemplating customer relationship and marketing functions getting more value through a digital transformation.



Organisations are also looking to digital transformation as a key to innovation, growth, discovery and creation of new business opportunities. Digital technology is improving enterprise performance in game-changing ways. Technology has always been a critical lever in improving operations, but the emergence and maturation of RPA and AI enables organisations to reach new heights when deployed effectively in operations. Somewhat surprisingly, even 'traditional' companies are leveraging data and AI in innovative ways. Implementing these technologies has benefitted these companies by reduced costs and increased profits, improved productivity and service delivery, improved time efficiency, etc.

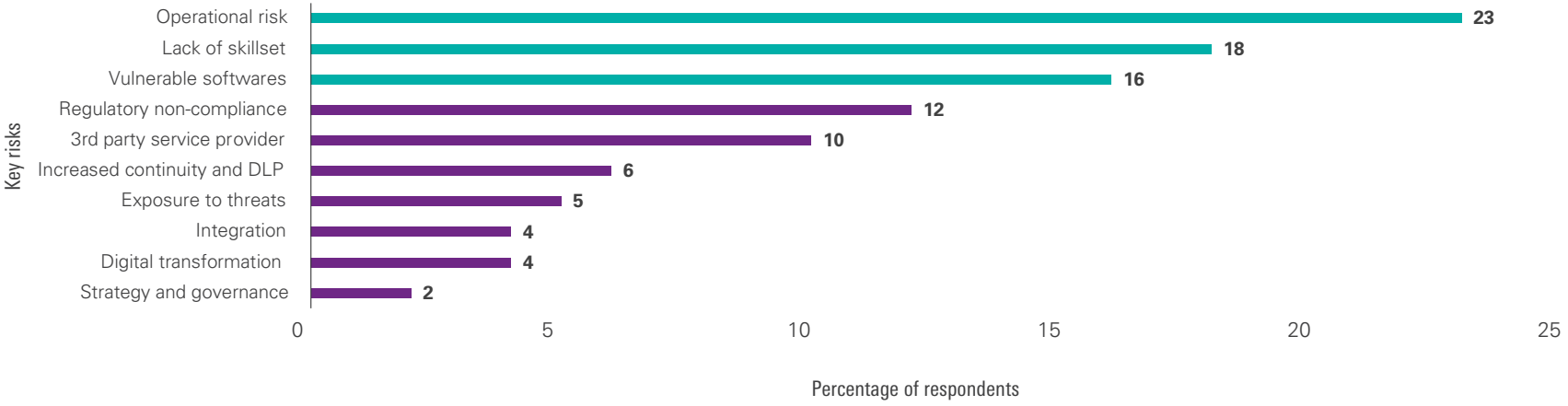
Several organisations are now developing and implementing chat-bots and other smart assets that gather client, economic, social and other internal data to formulate customised marketing and service recommendations improving customer relationship management. Customer acquisition, customer experience, and customer retention has become even more integral. Digital marketing changes not just how you service a customer and in terms of the brand perception, but it also changes the types of experiences and immediacy of experiences that you can deliver to customers. It changes the way you alter campaigns in the process, because you understand the impact of context in those campaigns[2].

2. How Digital Transformation Is Impacting Sales Service And Marketing, Tricia Morris, Customer think, November 2016
How to achieve operational efficiency through digital transformation?, Rakesh Kumar and Kinshuk Jhala, NASSCOM, November 2017



Top digital risks

In the journey of digital transformation, top three risks vary from organisation to organisation basis their scale of operations. However, basis our survey, a majority of the organisations consider operational risk at 23 per cent, lack of skillset at 18 per cent and vulnerable softwares at 16 per cent, as their top three risks.



While the top three digital risks are dynamic as per the needs of the organisation, the biggest risk will be a failure to detect the risks and to proactively work on the mitigation in order to avoid significant business impacts.

> With the evolution in cyber threat landscape, organisations need a crisis management plan. Since cyber security risk has become business risk, integration of business continuity plan (BCP) with the cyber crisis management plan makes more sense. The importance of BCP, which used to focus more on functional attributes has changed to impact due to cyber security. Therefore, in some organisations, the business continuity role lies with the CISO.
>
> **Sameer Ratolikar**
> Executive Vice President and CISO
> HDFC Bank

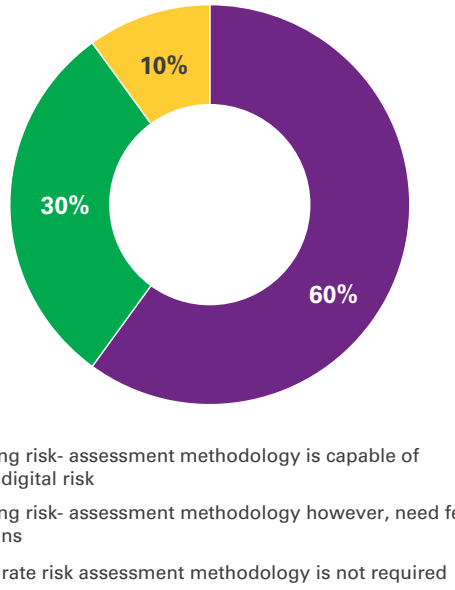
With the advent of digital transformation, it is not astonishing, that refining cyber security posture is of utmost priority for business and technology officials. It also appeals for the transformation in existing risk assessment methodologies to cope up with the new emerging digital risks. Artificial Intelligence (AI) and Machine Learning (ML) technology has emerged as an effective solution to manage these risks. It also provides a fascinating option, since the deep learning branch of AI allows machines to learn without human supervision. The power of this technology is always dependent on the amount of data that can be ingested, since deep learning output becomes more accurate as it receives more data. To leverage AI to the fullest, combining it with right security-intelligence personnel is necessary against several types of risks and attacks.

2 Digital risk: Assess, address and adopt

Digital risk: New age risk management frameworks

60%

of respondents suggest modifying existing risk management methodology to address digital risk



An organisation's risk assessment methodologies are evolving with the dynamic risk environment, managing risks effectively is a key challenge.

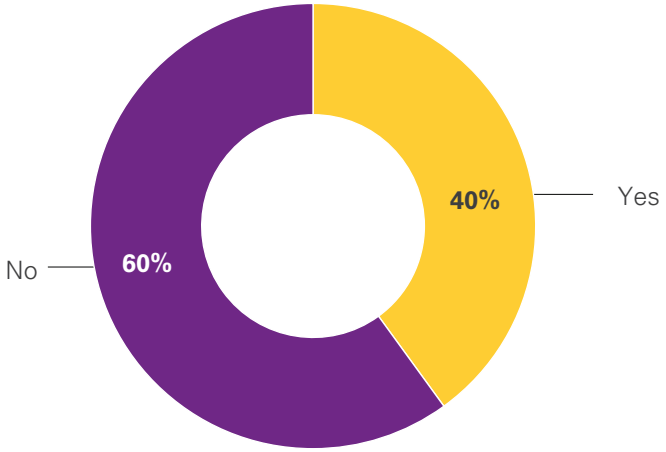
- Digital risk management should be a structured and disciplined business tool aligning strategy, processes, people, technology, and knowledge with the purpose of evaluating and managing the uncertainties that enterprises face.
- It should be holistic, integrated, future-focused, and a process-oriented approach that helps an organisation manage key business risks and opportunities with the intent of enhancing shareholder value for the enterprise as a whole.

KPMG in India believes that a holistic operational risk framework, which includes cyber security risk and digital risk as a foundational component, can help organisations achieve competitive advantage while securing the enterprise's most valued assets.

Digital risk: A separate risk domain

40%

of respondents currently treat digital risk as a separate risk domain



- Digital risk management has become the need of the hour as it affects business performance to a great level, if digital risks are not dealt with on priority.
- Mitigating and handling digital risks is the highest priority today for every digital business to shun off the impacts.
- Organisations are not entirely ready to defend themselves against the wave of emerging digital risks
- Integrating digital risk with the overall risk management framework is a preferred approach which needs organisation wide efforts and shift in culture of an organisation[3].

Survey results suggest that the industry is still evolving to consider and address digital risk as a separate risk domain altogether. While, there might be various reasons for the same, there is a need to have strong focus on digital risk arising out of various key factors such as adoption of newer digital technologies; redesigning of business models; business integrations and higher reliance on third party service providers and systems.

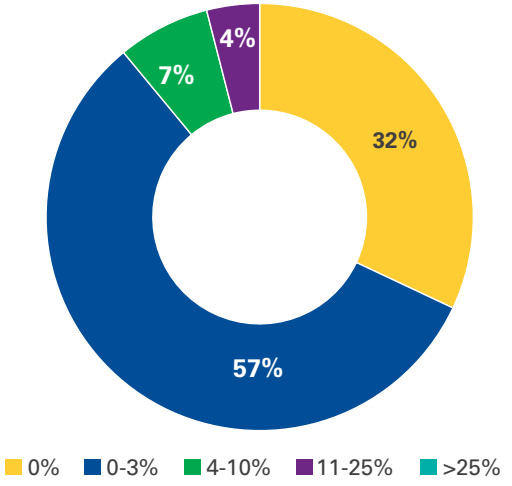
3. Recording Risk Riding The Ai Wave, KPMG UK, Andrew Shefford, January 2018
Lloyd's 360° Risk Insight Managing digital risk: trends, issues and implications for business, Lloyd's, 2010

Digital risk: Are we allocating requisite budget?

IT strategies of organisations are undergoing massive transformation with the advent of digital technologies. Almost, all the organisations are moving towards embracing digital technologies in their business operations, however, our study indicates that organisations are not allocating requisite budgets to address digital risks.

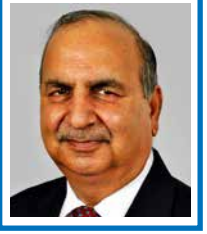
89%

of respondents suggest that less than 3 per cent of digital transformation budget is allocated to the digital risk domain



- Distribution of budget for digital transformation and percentage of budget allocated to manage digital risks is a critical factor in order to have successful digital transformation.
- Investments for digital transformation and managing digital risks should be distributed across strategic, tactical and operational levels.
- Organisations should invest in strategic factors like reskilling and up skilling of stakeholders including internal employees, investing in IT infrastructure, reinvesting risk management frameworks, etc.
- Investments in digital transformation and digital risk management should be monitored on a continuous basis and spending needs to be adjusted in order to achieve digital transformation along with managing digital risks.

> In the emerging business paradigm, both digital transformation and cyber security need to be planned simultaneously. Inadequate attention to cyber security could be detrimental for the digital journey. Organisations need to have an adequate maturity assessment framework to balance the two for desirable outcomes.
>
> **Rajesh Uppal**
> Senior Executive Director IT and CHRO
> Maruti Suzuki India

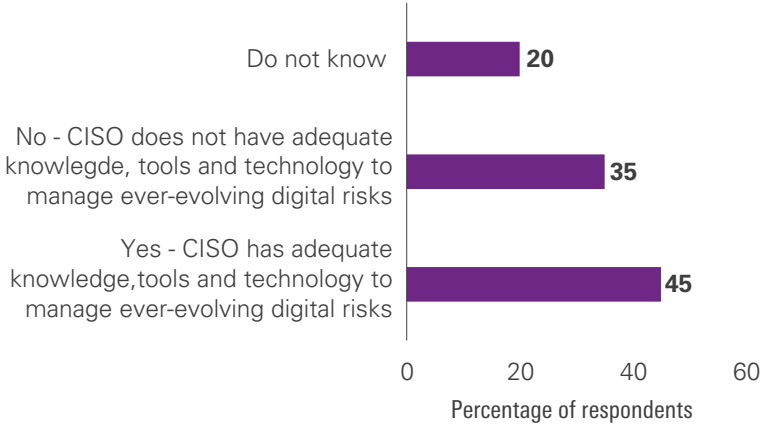


Digital risk: Skill enhancement

Organisations are split in saying that the Chief Information Security Officer (CISO) has adequate knowledge, tools and technology to manage ever-evolving digital risks versus does not have adequate knowledge, tools and technology to manage ever-evolving digital risks.

45%
of the respondents believe that CISO has adequate knowledge, tools and technology

35%
Believe otherwise



With the advent of digital transformation, it is no astonishment, that refining digital security is of utmost priority for business and technology officials. It brings out the need for upgrading the skillset and the existing tools which can help with the defence of emerging attacks in the digital world.

Most of the organisations are considering digital transformation as key to improve efficiency, enhance value delivery and stay ahead of the curve. However, organisations should increase focus on addressing digital risks as well along with digital transformation. Distribution of budget for digital transformation and percentage of budget allocated to manage digital risks is a critical factor in order to have successful digital transformation. Investments for digital transformation and managing digital risks should be distributed across strategic, managerial and operational levels.

Organisations should look for the right balance between quick return on investments and long-term strategic benefits. They should invest in strategic factors like reskilling and up skilling of stakeholders including internal employees, investing in IT infrastructure, reinvesting risk management frameworks, etc. Investments in digital transformation and digital risk management should be monitored on a continuous basis and spending needs to be adjusted in order to achieve digital transformation along with managing digital risks.

Organisations are increasingly adopting different measures to combat cyber security risks which include development of a comprehensive cyber security framework addressing cyber risk assessment, technology landscape, respond and recover strategies, cyber security awareness trainings, etc. Organisations need the framework which consists of standards, guidelines and leading practices to ensure that the critical infrastructure is protected. Security leaders have an obligation to identify and protect the organisation's 'crown jewels' – key business processes, intellectual property, enterprise and customer data, and market offerings. Organisations are looking to adopt a global framework which goes beyond ISO 27001:2013. Organisations are consciously moving forward to ensure that effective measures are established.

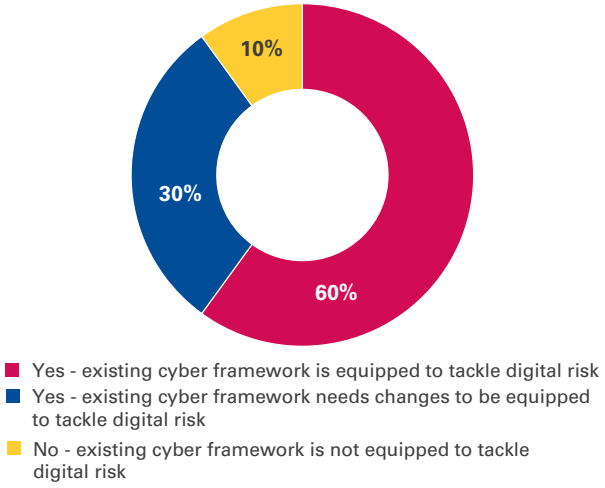
3 Digital risk: Defence and compliance

Digital risk: Enhance cyber security framework

Majority of the respondents feel that existing cyber security frameworks need to be enhanced to address digital risks to incorporate evolving digital risks

60%

of respondents stress on a need to enhance existing cyber security frameworks to address digital risks



- New technologies have transformed the risk landscape and have arisen a need for organisations to keep speed with the dynamic digital environment.
- Trends have shown a move from viruses or malwares to more criminals attempting to attack while going unnoticed.
- Attacks are becoming more complex day by day and digital technologies have become new targets for cyber criminals.

These technologies are extremely diverse and keep upgrading each day, therefore, enterprises should have a structure in place to help identify who presents a threat, how an attack might be mounted, where their technical vulnerabilities lie and how they would deal with an attack.

The team tackling digital risk for any organisation should keep a check on the emerging risks as an issue that is perceived to be potentially significant and keep upgrading their cyber framework based on the dynamic digital environment.

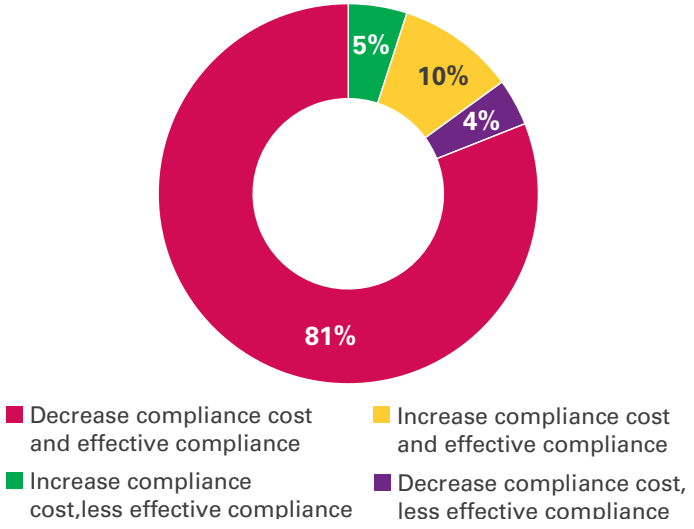
> Fourth industrial revolution has made digital future inevitable – it is the proverbial bus or vehicle that one cannot afford to miss. Cyber security is a cog in the wheel for this vehicle and has to be strong and resilient to move ahead on the unchartered paths, else we run the risk of disruption of this digital future. outcomes.
>
> **Rajeev Batra**
> CIO, Bennett Coleman and Co
> (Times Group)

Digital risk: Effective compliance management

Basis our survey results, majority of our respondents say digitisation will reduce the compliance cost, at the same time making compliance more effective.

81%

of respondents believe digitisation will reduce compliance cost, make compliance more effective



Key benefits of a digitised compliance management programme[4]

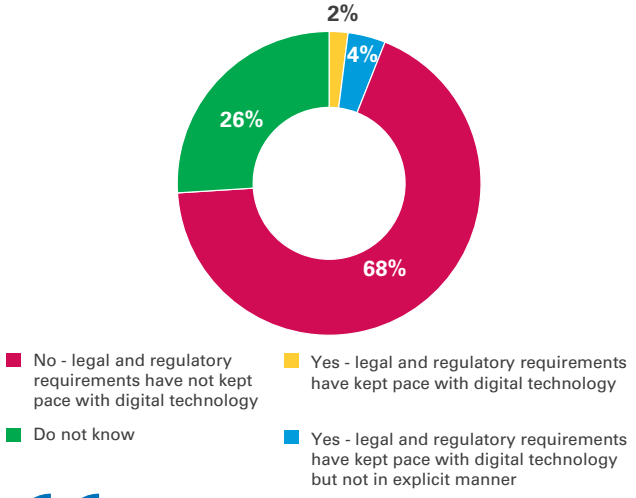
4. Continuous Auditing / Continuous Monitoring- Transformation Of Compliance, Governance, Risk And Compliance Services, KPMG in India, March 2019

Digital risks: Evolving regulatory landscape

While there has been a significant rise in the adoption of digital technologies by organisations, our survey indicates that organisations still believe that the current regulatory environment is not emulated with this dynamic technology change.

68%

of respondents stress on a need to enhance regulatory landscape to address digital risks



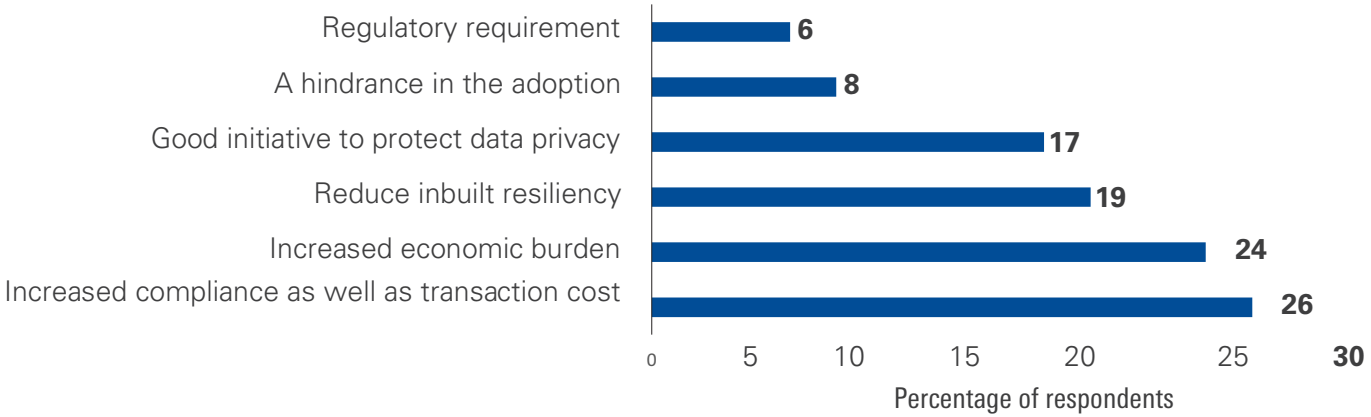
- Regulators across the globe should recognise their role in forecasting innovation and provide clear guidance around emerging digital technologies.
- Companies that are looking to use exponential technologies to create innovative business models should work with governments and stakeholders to develop regulations that are adaptive, transparent, and participatory, drawing on new models of collaboration between the public and private sectors.
- If this is executed then innovators will have the freedom to apply new digital technologies without regulatory disconnect holding them down.

> Compliance and regulatory scenario for most of organisations is a little foggy in nature. For organisations like ours who have operations across geographies, understanding regulatory requirements of various countries becomes a challenge. Often, we have to modify our business strategy on the go, which costs us financially. For organisations that are more stringent in compliance, awareness regarding many regulatory checkpoints is essential.

Satyajit Sarker
VP and Global CIO
OmniActive Health Technologies

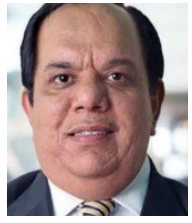
Digital risk: Data localisation

As organisations are becoming borderless as part of their expansion strategies, there has been a lot of pressure from a regulatory standpoint to comply with cross border restrictions. While few of our respondents considered it as good initiative to protect the consumer's privacy, some of the inputs also stated the perception increased economic burden along with transaction and compliance costs, and reducing resiliency capabilities through storing data locally.



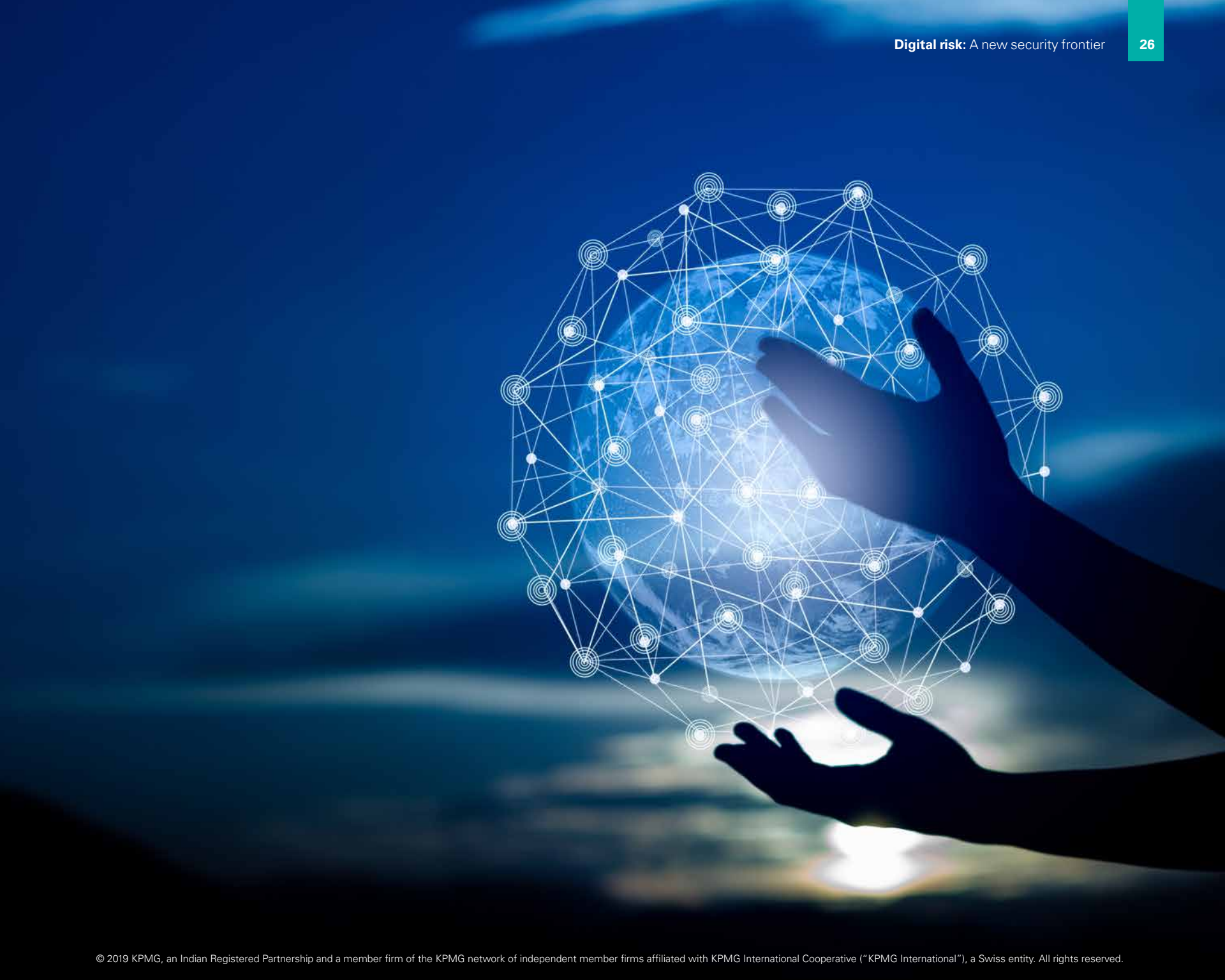
The government is progressively restricting cross border data flows in order to ensure security and privacy of the consumer's personal data. While, these data localisation measures will definitely aid in protecting the consumer's privacy and risks of cyberattacks, thereby increasing digital trust of a consumer, however, the impact of these requirements on economic and trade costs is likely to be considerable. The impression of restricting cross border data flow to non-adequate countries with low level of privacy protection is reasonable, to ensure adequate level of security control implementation for data protection. However, data localisation will not only fail to achieve this, it also adds to additional cost of implementation for storing data locally and reduce resiliency capabilities of an organisation to a great extent[6].

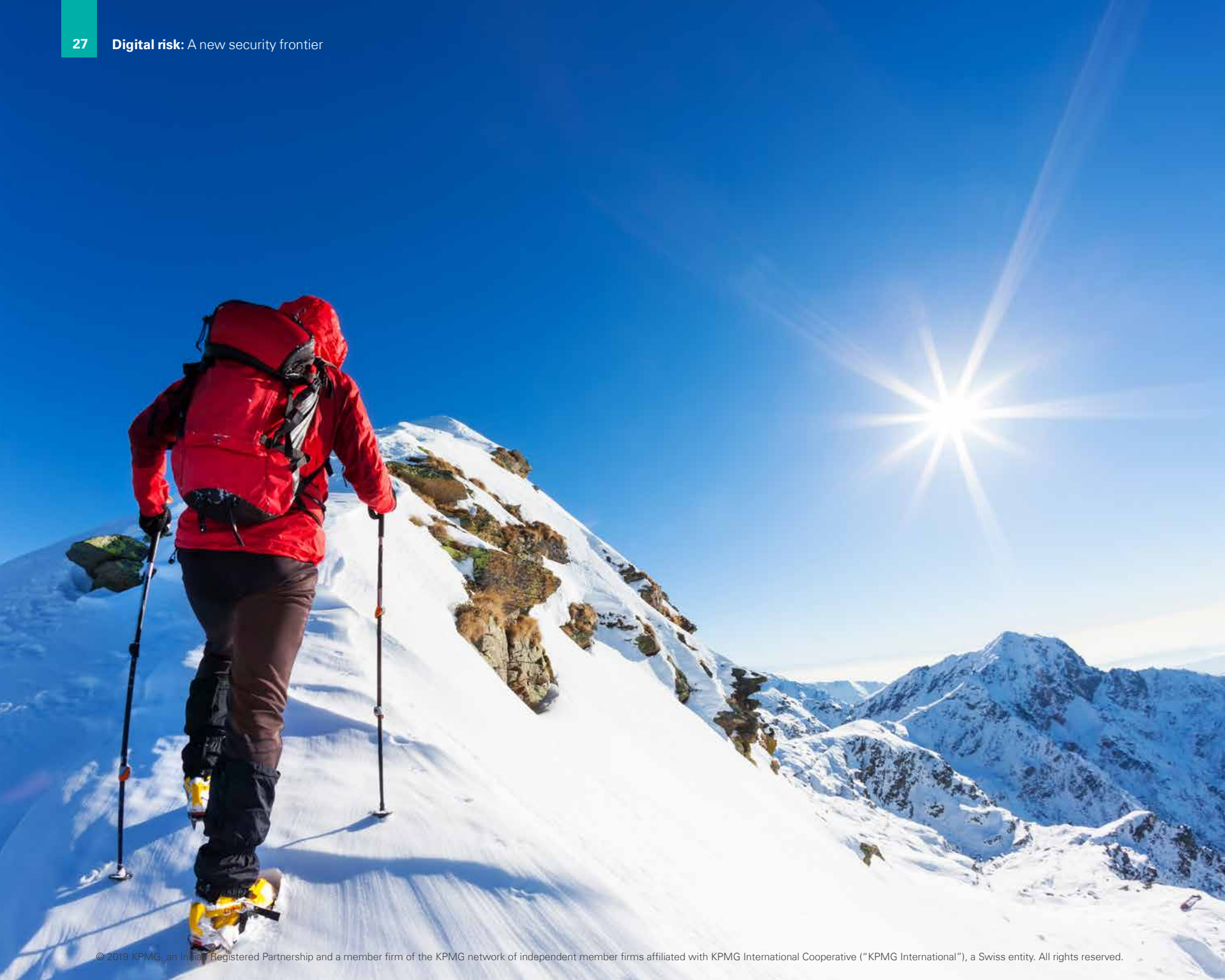
> With digital footprint expanding the organisational boundaries into a borderless world, digital risk management requires to transcend beyond the traditional ways of managing IT risks. Organisations need to design holistic risk management framework that encompasses data integrity and customer privacy at its core in order to secure their digital assets.
>
> **Vijay Sethi**
> Chief Information Officer, CHRO and Head of CSR
> Hero MotoCorp Ltd



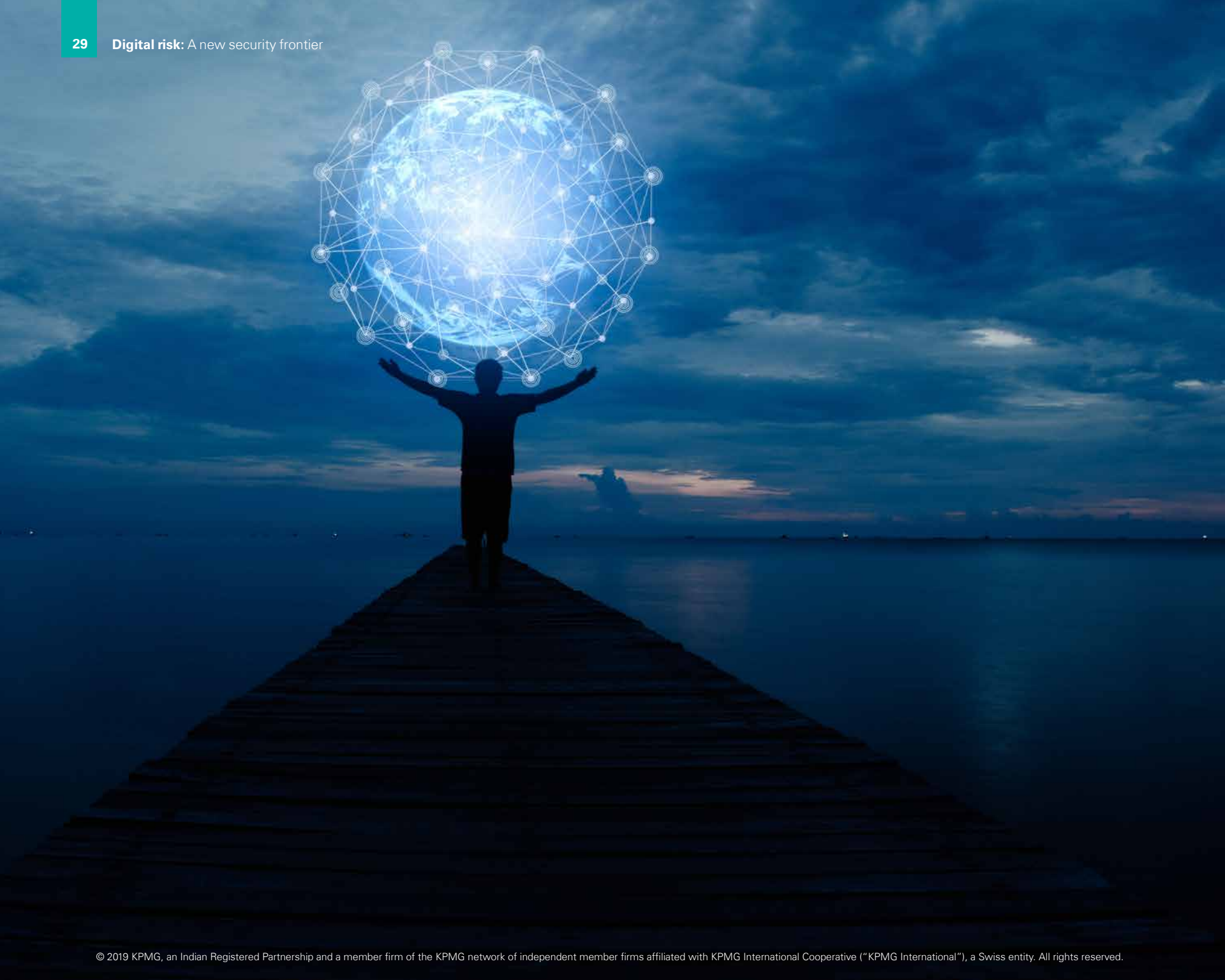
Digital transformation programmes are also automating compliance programmes. Organisation wide compliance management programmes are likely to bring in more effectiveness while reducing overall compliance cost. However, compliances which push through various regulatory channels can have overall impact on the digital transformation strategy and associated digital risk due to various reasons such as data localisation; data access to country specific regulators/nodal agencies, cross border data sharing protocols. In any case, organisations will need to have sound cyber security/digital risk frameworks and effective compliance management programmes.

5. Continuous Auditing / Continuous Monitoring- Transformation Of Compliance, Governance, Risk And Compliance Services, KPMG in India, March 2019 and Peter Lovelock, March 2018





Way forward



The rampant pace of adoption of digital technologies is being analysed to provide significant benefits, but this has considerably altered the risk profile of a country, organisations, businesses and individuals.

The new age digital technology has led to deployment of services in near real time environment which has challenged the traditional way of building technology and then securing it.

This brings forth some key questions:

1. Are we ready to deal with digital risks associated with adoption of new age technology or we will learn only by making mistakes?
2. Have we thought of all aspects sufficiently when securing new age technologies or are we ignoring them as we increase the pace of embracing them for our benefits?
3. Do we have required skilled resources to assess, address and adopt digital risks?
4. Are we equipped with the requisite set of tools, technologies or methods to address the risks we face currently and which continue to multiply by thenNano second?

Three simple, yet effective takes on managing digital risks:

1. **Develop an agile risk management framework with the clients/ consumer at the centre**
2. **Establish an effective governance model and drive the tone from top.**
3. **Develop a wider perspective and a more inclusive approach since risks are constantly changing – and change is the only constant**

To manage digital risks, we need to think differently. With a different mind-set and approach.

At KPMG in India, we focused on bringing relevant approachsolutions such that the organisation can focus on the benefits and the risks simultaneously get managed. We have been investing in this area, specifically on the following:

1. **Established thorough risk framework** – thorough risk management approach integrated with corporate governance requirements
2. **Artificial Intelligence (AI) in control** – aimed at helping clients make responsible and transparent use of these powerful tools, ensuring alongside that appropriate governance and assurance is in place. One of the key areas in which we are working is 'adoption of RPA'. Today, RPA has become a realistic methodology intended to provide tactical benefits and allows organisations to concentrate on strategic approaches on a larger scale. Automation is the new norm in the business and the subsequent risk disrupts innovation. With the future of business being managed using Artificial Intelligence (AI), Machine Learning and Deep Learning, auditing/assurance of these emerging technologies is becoming more complex than a customary technology audit.
3. **Digital insight protection platform** – helps generating deeper insights on the risk exposure of an organisation emanating from digital technologies. Use of digitalisation and power of digital technologies to enhance the 'risk management' domain
4. **Digital risk platform** – The area of risk management is a big benefactor of digitalisation in recent years. This has allowed businesses/risk professionals to harness the power of technologies to:

1. Work on larger volume of data;
2. Move away from reactive risk assessment to predictive risk management;
3. Implement risk quantification models and explore actuarial sciences;
4. Perform effective and consistent risk management through historical data analysis; and
5. Use risk management to provide deep insights and bring much needed efficiencies.

Our 'Digital risk platform' is specifically built to harness the power of digital technologies and utilise it for deeper, insightful risk management activities as mentioned above.

About the survey

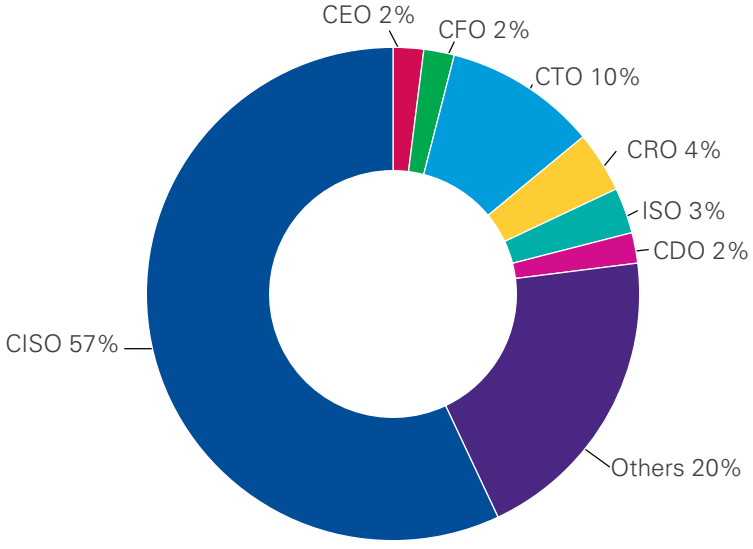
We recently conducted a survey with an aim to provide the industry with a reference point that provides corporate and end users' perspectives on the fast-changing nature of digital channels and how organisations cope up with this rapid digitisation.

This survey seeks views from various customers and users across different sectors on cyber security and technology risk management. The contents of the survey is derived from the responses of the participants and is complemented by insights from our experts in technology risk management.

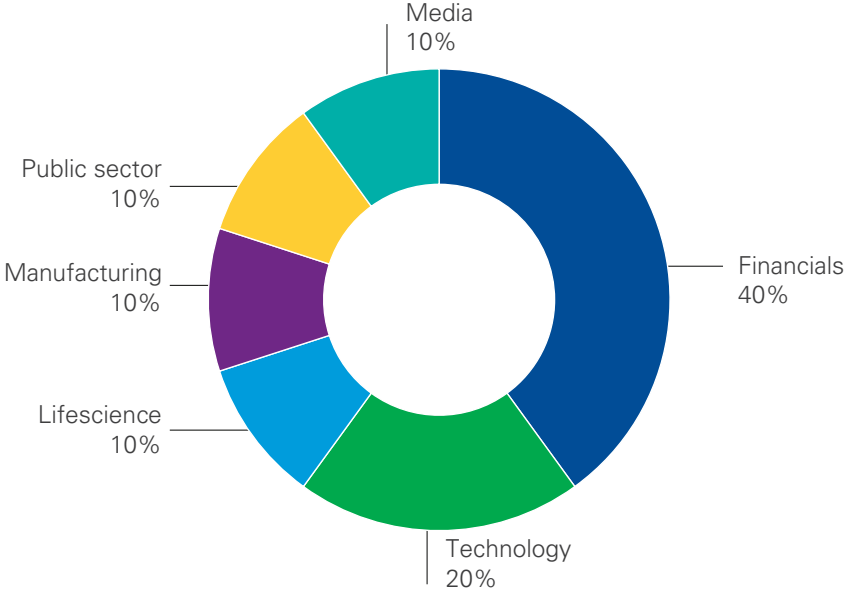
An overview of demographics of survey participants: Profile of participants

The survey saw over 350 participants across designations and different sectors who are in the profession of technology risk management in India.

Profile of respondents



Industry representation



About Grey Head Media

Incorporated in 2011, Grey Head Media is a promising B2B enterprise technology media organisation facilitating inter and intra-community dialogue for various professional groups including CIOs and CISOs in the entire South Asian region.

Using its time-tested mediums of confluence, content and collaboration, Grey Head Media today continues to extensively engage with sub-continent's prominent C-suite executives in both information technology and information security domains.

The core belief of the group is that these communities are fiercely protective about their distinct identities and do not want to be clubbed with an amorphous pool of professionals, and therefore Grey Head strives to be a dedicated catalyst promoting community interactions on totally neutral platforms. Our focus is on creating rich, engaging platforms that enable both intra- and inter-community dialogue.

With established credentials, proven track record, and remarkable backing from both partners, and communities, Grey Head Media continues to establish new benchmarks in the industry.

About KPMG in India

KPMG in India, a professional services firm, is the Indian member firm affiliated with KPMG International and was established in September 1993. Our professionals leverage the global network of firms, providing detailed knowledge of local laws, regulations, markets and competition.

KPMG has offices across India in Ahmedabad, Bengaluru, Chandigarh, Chennai, Gurugram, Hyderabad, Jaipur, Kochi, Kolkata, Mumbai, Noida, Pune, Vadodara and Vijayawada. KPMG in India offers services to national and international clients in India across sectors. We strive to provide rapid, performance-based, industry-focussed and technology-enabled services, which reflect a shared knowledge of global and local industries and our experience of the Indian business environment.

KPMG in India Cyber Security services

Strategy and governance	Cyber transformation	Cyber defence	Cyber response
Helping clients align their cyber agenda with dynamic business requirements and compliance	Helping organisations to transform cyber posture by driving cyber programmes	Provide greater visibility and understanding of technical risks	Helping clients with effective and efficient response to cyber incidents, forensic analysis and detailed investigations

Digital Cyber security – Cloud | Mobile | Internet of Things | Intelligent Automation |Blockchain- high value manged services

Acknowledgements

We would like to thank the following people for their continued support and guidance during the development of the report.

For KPMG in India: Business team

Atul Gupta
Mubin Shaikh
Zubin Mehta
Rohit Walke
Harshad Joshi
Neha Randive
Anshuman Bhalla
Abhijit Barve
Iqra Bhat

For KPMG in India: Design and compliance team:

Anupriya Rajput
Rahil Uppal
Sharon D'silva

For Grey Head Media:

Rahul Neel Mani
Shipra Malhotra
Muqbil Ahmar
Robin Chatterjee

KPMG

KPMG josh

IT SHOWS

IN OUR ABILITY TO TRIUMPH OVER ANYTHING IN OUR SPIRIT OF UNDYING ENTHUSIASM OUR DRIVE TO ACHIEVE THE EXTRAORDINARY UNMOVED BY FEAR OR CONSTRAINT WE'RE DRIVEN BY JOSH AND IT SHOWS

THIS ADVERTISEMENT FEATURES KPMG INDIA EMPLOYEES

KPMG in India contacts:

Nilaya Varma
Partner and Leader
Markets Enablement
T: +91 124 669 1000
E: nilaya@kpmg.com

Akhilesh Tuteja
Partner and Head
Risk Consulting
Global Co-lead – Cyber security
T: +91 124 336 9400
E: atuteja@kpmg.com

Atul Gupta
Partner and Head
IT Advisory;
Cyber security Leader
T: +91 124 307 4134
E: atulgupta@kpmg.com

Mubin Shaikh
Partner
Cyber security - IT Advisory
T: +91 206 747 7018
E: mubin@kpmg.com

Grey Head Media contact:

Rahul Neel Mani
Co-Founder and Editor
T: +91 9958499636
E: rahul.mani@greyhead.in

#KPMG josh

Follow us on:
kpmg.com/in/socialmedia

This document is for e-communications only. (067_THL0316_AR)