



The Changing Face of Digital Analytics
Page 14



Managing Data Risks with Internal Audit Support
Page 38



Raising the Digital Competency of the Board
Page 48

SID-SMU DIRECTORSHIP PROGRAMME

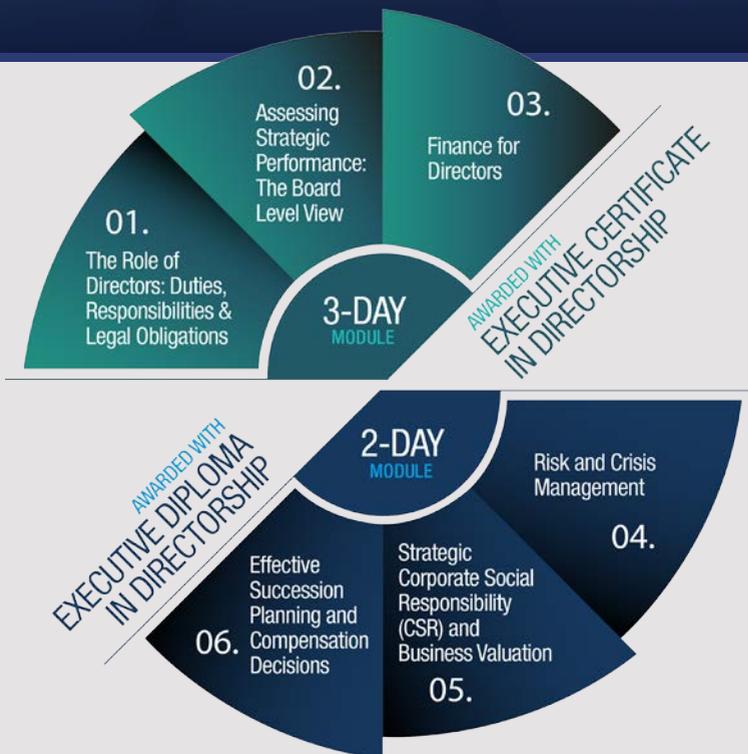
CREATING EFFECTIVE BOARD LEADERSHIP

“ A board must be collectively confident and steadfast regardless of the company's situation. The structural tools to achieve this are delivered in this course. I had the privilege of learning from a renowned and remarkable faculty. In my view, it is a “must” for Singapore directors.

With lecturers from academia and the industry, it was a truly balanced and practical programme. Additionally, with participants from MNCs, government, business entrepreneurs and professionals, the value of the networks and relationships alone far outweighs the cost of the programme.

”

DR WILSON CHEW
Partner, PwC Singapore



Executive Skills for Board Members in Challenging Times

PROGRAMME DETAILS

The directorship programme is first of its kind in Singapore with a formal certification process, focusing on director training.

PROGRAMME STRUCTURE

The programme is organised in two tiers. Participants have the option to obtain an Executive Diploma in Directorship upon completion of six assessable modules, or the Executive Certificate in Directorship, which consists of three assessable modules (Module 1, 2 and 3).

Singapore Management University, Executive Development

Get in touch with our advisor, David Lim at davidlimbp@smu.edu.sg or +65 6808 5393. You may also visit <http://exd.smu.edu.sg>

Singapore Institute of Directors

SID Secretariat Email: events@sid.org.sg | www.sid.org.sg | Tel: +65 6422 1188 | Fax: +65 6422 1199

The New Black Gold



By **PAULINE GOH**
Chair, SID Bulletin Committee

Data, in particular, big data – as in the massive volume of structured and unstructured data that is growing at ever-increasing rates – is often referred to as the new oil.

That's because being able to harness its power – through data analytics and a host of exponential technologies – is fast becoming the most competitive advantage in business. Even for companies that have resisted this type of change, it is becoming impossible to ignore the opportunities big data presents.

In this issue, we look at the phenomenon of big data and its impact on businesses and board governance.

We kick off with an at-a-glance overview by Howie Lau of the growth, value, risks and protection of data, as well as the people and organisations most involved with big data processing and management (page 6).

Making sense of the growing reservoir of untapped data and information amassed is another matter. According to some research, less than 20 per cent of all the data collected by organisations is used. How can organisations address this huge potential of information?

Stephen Raj looks at the evolution of data and how data analytics is driving enterprise



DIRECTIONS

performance and growth (page 14), while Lee Joon Seong and Khoong Hock Yun look at the domains of artificial intelligence and distributed ledger technology respectively (pages 18 and 22).

From the board's perspective, the operational aspects of big data may seem a shade too much to digest, and best left to management and data scientists. But it is increasingly hard to avoid the responsibilities of having in place proper data governance and data protection, security and strategies in the organisation. The benefits – and the penalties (operational, financial and reputational) are significant.

Mr Sid makes this point in his response to a director's concerns (page 58). Other writers look at various aspects of the board's role in this area: Philip Chong provides a framework for data governance (page 44), Lee Shih Yen provides a checklist for boards in their evolving role in cyber security management (page 54), and Lyn Boxall shares on the attitude needed for data protection (page 56).

As the trend of big data continues to grow, the focus will shift towards wider adoption across more industries and harnessing data for the greater good. Meanwhile, enterprises which ramp up the groundwork towards this vision are going the extra mile in search of the right data. Are you in for the count? ■

SID

SINGAPORE
INSTITUTE OF
DIRECTORS

SID Bulletin Committee

CHAIR

Pauline Goh

MEMBERS

Adrian Chan
Willie Cheng
Robert Chew
Philip Forrest
Kevin Ho
Howie Lau
Victor Yeo

PUBLISHER

Singapore Institute of Directors

#11-03 Capital Tower

168 Robinson Road

Singapore 068912

Tel: +65 6422 1188

Fax: +65 6422 1199

Email: secretariat@sid.org.sg

Website: www.sid.org.sg

We are now on **LinkedIn**

EDITOR

Yang Wai Wai

EDITORIAL COORDINATOR

Sue Anne Kuek

DESIGN

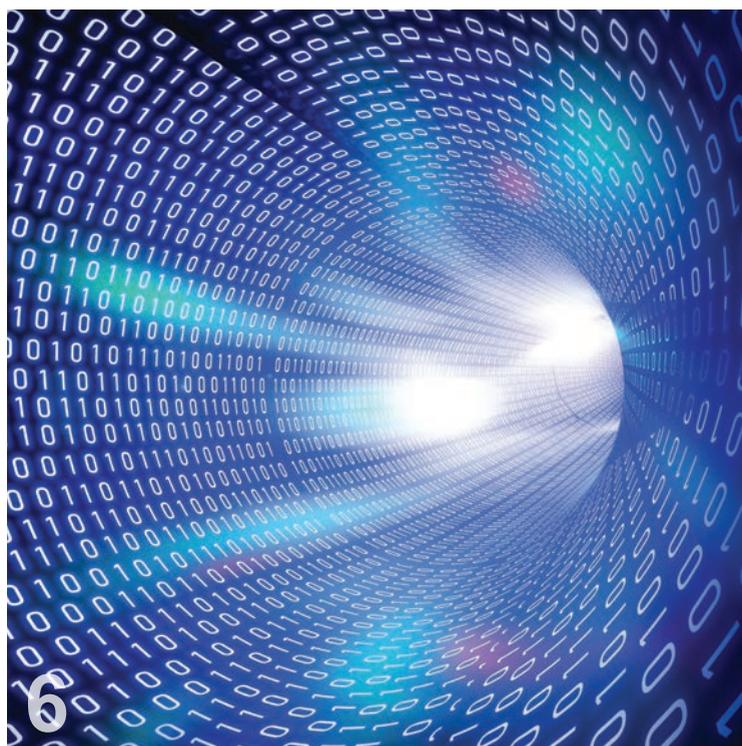
Epiphany Design

PRINTER

Entraco Printing Pte Ltd

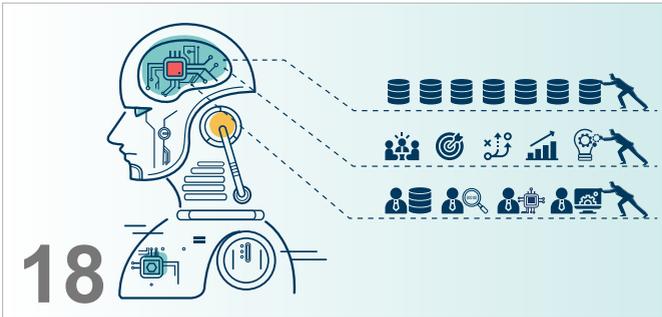
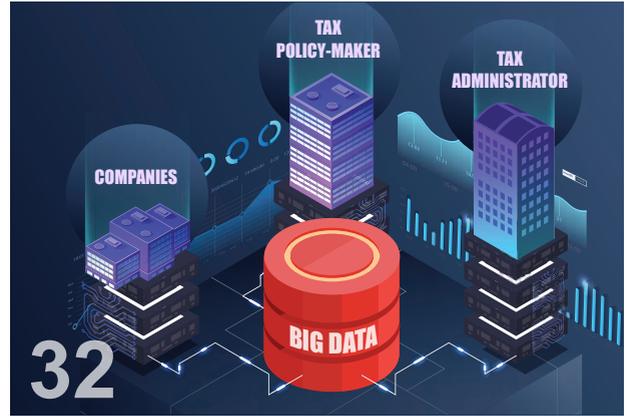
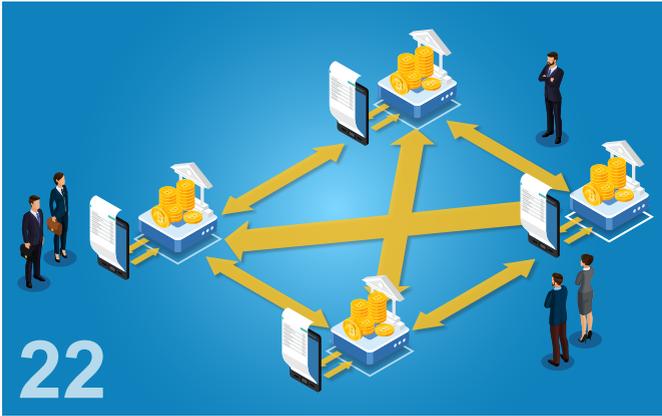
For ease of reading, the male gender is used in the Bulletin to refer to all personnel unless the context specifically requires otherwise.

CONTENTS



FEATURES

- 6 Data, Data, Data
- 14 The Changing Face of Digital Analytics
- 18 Delivering AI at Scale
- 22 Improving Corporate Governance with Distributed Ledger Technology
- 28 Can Pofma Protect Businesses?
- 32 Taxation in the Global Spider's Web of Big Data
- 38 Managing Data Risks with Internal Audit Support
- 42 Burgeoning Demand for Data Centres in Asia Pacific
- 44 Data Governance and the Board
- 48 Raising the Digital Competency of the Board
- 54 The Evolving Role of the Board in Cyber Security



COLUMNS

- 36 COUNTING BEANS
The Accountant and Big Data
- 56 BOARDROOM MATTERS
Data Protection – Taking the “It Will Happen” Approach
- 58 ASK MR SID
Too Much Data About Data

INDUSTRY NEWS

- 62 The AC Seminar 2020:
Looking Beyond the Veneer of Numbers
- 72 Global Director Survey
- 77 Director Appointments

SID CALENDAR

- 79 SID’s Q1 Events (Jan–Mar 2020)
- 80 Upcoming Events

SID NEWS

- 75 Cutting Through the Complexity of Risk Management
AC Pit-Stop: Managing Risk in a Digital World
- 76 SGOOD Advanced: Developing a Digital Mindset
SGOOD Advanced: Branding for NPOs
- 78 Photo Gallery
- 86 Welcome to the Family

DATA, DATA, DATA

By **HOWIE LAU**
Chief Industry Development Officer, Infocomm Media Development Authority



Data is everything and everywhere in today's world.

It is a digital tsunami that can be overwhelming to each of us and our organisations.

It is a gold mine to be explored for the insights and intelligence it can provide on customers and other stakeholders.

It is a danger trove of personal and corporate information that can be misused and abused.

Love or hate it – we have to deal with it.

The infographics on the following pages explore the different facets of data:

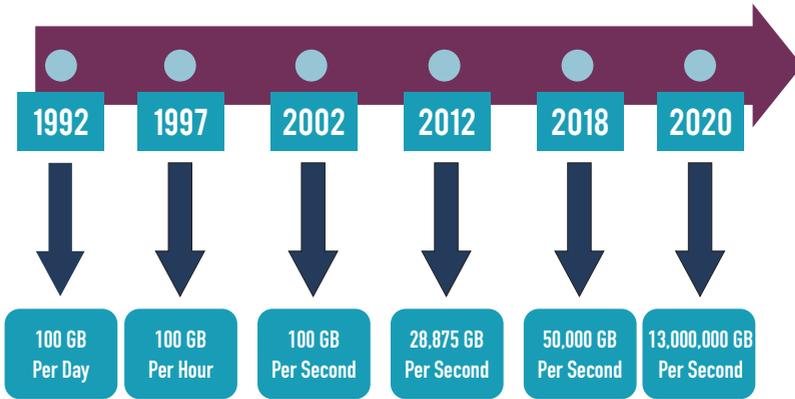
- Data growth
- Data value
- Data risks
- Personal data protection
- Data people
- Data organisations

Data Growth



Data volume has skyrocketed. More data was generated in the last two years than in the entire human history before that.

Moving Towards Big Data



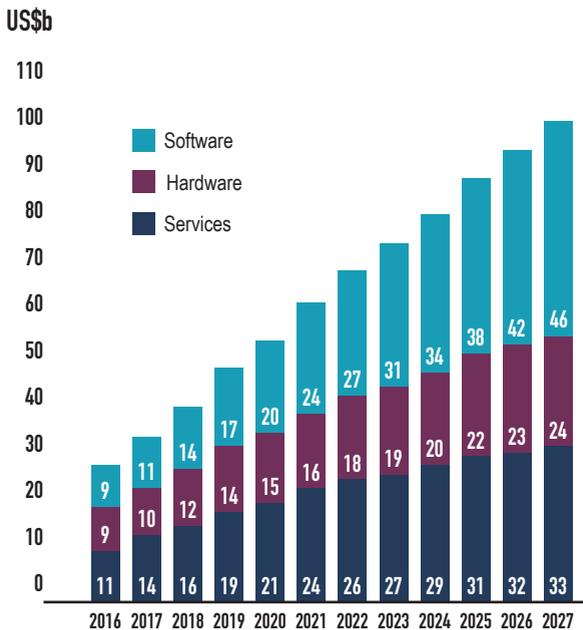
Source: Domo; Rahul Anand, Quora

Know your Bytes

- Kilobyte ————— KB
- Megabyte ————— MB
- Gigabyte ————— GB
- Terabyte ————— TB
- Petabyte ————— PB
- Exabyte ————— EB
- Zettabyte ————— ZB
- Yottabyte ————— YB

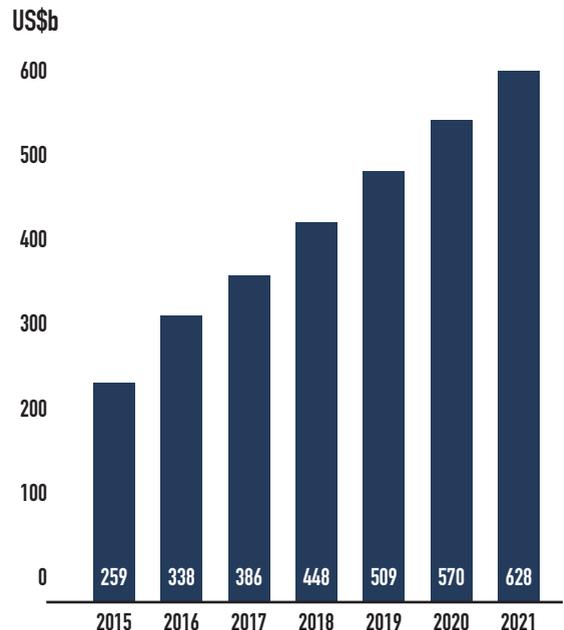
Each layer is 1000 times more than the one above.

Big Data Revenue Worldwide



Source: Statista (figures from 2019 onwards are forecasted)

Number of Hyperscale Data Centres Worldwide



Source: Cisco Systems Inc (2018 figures onwards are forecasted)

Data Value



Data in itself brings little value. Value is created from the relevant use of data, in particular, insights derived from the data analytics and acted upon.

The Insights Value Chain

Technical foundations			Business foundations							
Data	X	Analytics	X	IT	X	People	X	Processes	=	Value captured
New data sources		Descriptive statistics		Cloud sourcing		Culture change		Adaption business processes		The insights value chain is multiplicative, i.e. you are only as good as the weakest link in the chain
Orchestration of data		Classical predictive statistics		Horizontal scaling (No-SQL, Hadoop)		Data-enabling decision making		Automation business processes		
Unstructured data		Machine learning		Analytical programme languages		Role profiles		Data and analytics governance		
Privacy and legal considerations		Cognitive modelling		Data visualisation		Organisation		Cross-functionality		
Data security		Optimisation		In-memory analytics		Analytics talent		Agile processes		
		Simulation		IT stack				Ecosystem management		

Source: McKinsey & Company

Gains from Analytics Deployment

- Improved efficiency and productivity **64%**
- Faster, more effective decision making **56%**
- Better financial performance **51%**
- Identification and creation of new product and service revenue **46%**
- Improved customer acquisition and retention **46%**
- Improved customer experiences **44%**
- Competitive advantage **43%**

Source: 2020 Global State of Enterprise Analytics (MicroStrategy)

Data Tools

Machine Learning. Makes it possible to quickly and automatically produce models that can analyse more complex data and deliver fast, more accurate results – even on a very large scale.

Data management. Ensures reliability and quality of data through good governance, standards and repeatable processes.

Data mining. Examines large amounts of data, sifting through the chaotic and repetitive noise to pinpoint relevant information to accelerate the pace of informed decision making.

Hadoop. Stores large amounts of data and run applications on clusters of commodity hardware. Hadoop's open source framework is free.

In-memory analytics. Derives immediate insights from data sitting in memory, and allows organisation to stay agile and act quickly.

Predictive analytics. Uses historical data, statistical algorithms and machine-learning techniques to identify likely future outcomes in fraud detection, risk, operations and marketing.

Text mining. Analyses text data from the web, comment fields, books and other text-based sources combined with machine learning and language processing to uncover hitherto unknown insights.

5G. Increases dramatically the speed of data transmission and data traffic not only from smartphones but the Internet-of-Things enabled devices.

Data Risks

The loss and misuse of data is an increasing risk for organisations. The surface area of cyber attacks and data breaches have increased with increased connectivity of people and organisations. The governance of data risk requires a dedicated focus on and balance of data privacy, data rights, technology and trust.



Data Security Statistics

- > **1.76 billion** records leaked in January 2020 alone.
- > **US\$3 trillion** – the global cost of cyber crime.
- > **76%** of cyber attacks are financially motivated.
- **48%** of all data breaches are malicious or criminal attacks.
- **US\$11.5 billion** – the cost of ransomware to businesses.
- **70%** of businesses are not prepared to respond to a cyber attack.
- **US\$3.6 million** – the global average cost of a data breach.
- **91%** of cyber attacks are through phishing emails.



Data Breaches In Singapore

- **Mindef hacked (2017)**
Hackers got away with personal data of 850 NSmen only as Mindef keeps its information on a separate server. Attack was premeditated and could be state-sponsored.
- **Singhealth cyber attack (2018)**
1.5 million SingHealth patients, including the Prime Minister, had their personal particulars stolen. A state actor is suspected.
- **HIV data leak (2019)**
Confidential information of 14,200 HIV-positive individuals were posted online in January 2019. Mr Farrera-Brochez who was previously convicted of fraud and drug-related offences was suspected to have leaked the information.
- **Accounts sold on dark web (2019)**
A Russian cyber security group found usernames and passwords of accounts related to MOH, MOE, Singapore Police and NUS and payment card details on the dark web.
- **Blood-donors' personal information exposed (2019)**
Over 800,000 blood donors had their information leaked online due to a loophole in the system. A cyber security expert spotted the fault, and Health Sciences Authority disabled the database.



Data Security Measures

- **Improve data protection and prevent data compromise.** For example, protect stored data directly so that it is unusable even if extracted.
- **Improve detection and response to data incidents.** For example, designate a data officer to monitor and analyse data incidents that pose significant harm.
- **Raise competencies and instil a culture of data awareness.** For example, conduct data security training regularly.
- **Account for data protection at every level.** For example, to consider third party vendors in the handling of data.
- **Ensure continuous approach to data security.** For example, levelling up on inhouse and outsourced expertise.

Source: Cyber Security Statistics 2020, The Best VPN.

Personal Data Protection

Data privacy and confidentiality are important to individuals concerned. The law requires the protection and accountability of personal data obtained, processed and stored by organisations. The PDPC offers a suite of accountability tools to help organisations with their personal data protection needs.

Legislation

Personal Data Protection Act (PDPA)

- The PDPA is the principal data protection legislation enacted in Singapore in 2012.
- Act sets out obligations for collection, use, disclosure, access, correction, care, protection, retention and transfer of personal data by all private sector organisations.
- “Personal data” defined as: data, whether true or not, about an individual who can be identified (a) from that data or (b) from that data and other information accessed.
- The national Do Not Call (DNC) Registry allows individuals to register their Singapore telephone numbers to opt out of receiving marketing phone calls, mobile text messages (SMS, MMS), and faxes from organisations.
- PDPA administered and enforced by Personal Data Protection Commission (PDPC).
- Mandatory to appoint a Data Protection Officer (DPO), optional to register DPO with the PDPC.
- Penalties for various forms of breaches under the Act. In 2019, PDPC fined 50 organisations a total of \$1.54 million for data breaches. The maximum fine of \$1 million was for the SingHealth breach.

Other legislation impacting personal data

- Computer Misuse Act (unauthorised access, modification and use of computer material).
- Cybersecurity Act (cybersecurity policies and standards. owners and operators of critical information infrastructure)
- Spam Control Act (bulk sending of unsolicited commercial emails).
- Banking Act (banking secrecy).
- Telecoms Competition Code (end-user service information by licensees).
- Private Hospitals and Medical Clinics Act (confidential medical information and retention of medical records).
- Regulations for financial sector issued by Monetary Authority of Singapore.

Accountability Tools

Guide to Data Protection Management Programme (DPMP)



Guide to Data Protection Management Programme (DPMP)

- DPMP Guide available from PDPC.
- DPMP is a systematic framework to help organisations establish a robust data protection infrastructure.
- Covers management policies and processes as well as roles and responsibilities of people in the organisation in relation to personal data protection.
- Helps organisations build high-trust relationships with customers and business partners through its ability to demonstrate accountable practices.

Data Protection Trustmark (DPTM)



- Certification of Trustmark administered by IDMA.
- DPTM is visible badge of recognition that organisations are accountable and responsible in their data protection policies and practices.
- Will help businesses increase their competitive advantage and build trust with their customers and stakeholders who will be assured of adequate data safeguards and contingency actions in event of breach.
- More than 20 DPTM-certified organisations as of 29 February 2020.

Trusted Data Sharing Network



- Launched in June 2019 to facilitate trusted data sharing between organisations.
- Helps to establish baseline practices for a systematic approach to trusted data sharing partnerships.
- Provides guidance for organisations to negotiate in four key areas:
 - o Data sharing strategy
 - o Legal and regulatory considerations
 - o Technical and organisation considerations
 - o Operationalising data sharing

Data People



The growth of data has resulted in the need for a workforce that can work with the challenges and opportunities created by the massive amounts of data. The field is generally known as data science and analytics (DSA). But beyond the DSA professionals, there’s also a demand for data leadership and an aptitude for analytical data decision making in management.

Data-driven leadership

- **Directors.** The board as a whole needs to understand the value of data and set the tone for its protection and exploitation for business benefit.
- **Senior management.** In the digital era, business leaders must be able to sift through the deluge of data to make good informed decisions. The demand for data-driven decision makers, such as data-enabled marketing managers, will comprise one-third of the data savvy professional job market in the US.
- **Chief Data Scientist.** There is a requirement for senior analytics leadership to set the vision, prioritise the roadmap, advocate and manage stakeholders on the data journey.
- **Data Protection Officer.** This is a mandated position to ensure the continued compliance with PDPA and other data protection responsibilities.

Data Science and Analytics Professionals

- The demand for DSA skills is exploding. In the US, there will be 2.7 million DSA job openings in 2020.
- Supply is however lagging demand. DSA jobs remain open five days longer than average.
- Organisations should build, not just hire, their data muscles. There are training programmes such as the TechSkills Accelerator for upskilling the workforce.

Types of DSA Jobs

	DSA Framework Category	Functional Role	Sample Occupations
↑ Analytical Rigor	 Data Scientists & Advanced Analytics Professionals	Create sophisticated analytical models used to build new datasets and derive new insights from data	Data Scientist Economist
	 Data Analysts	Leverage data analysis and modeling techniques to solve problems and glean insights across functional domains	Data Analysts Business Intelligence Analyst
	 Data Systems Developers	Design, build and maintain organisation's data and analytical infrastructure	Systems Analyst Database Administrator
	 Analytics Managers	Oversee analytical operations and communicate insights to executives	Chief Analytics Officer Marketing Analytics Manager
	 Functional Analysts	Utilise data and analytical models to inform specific functions and business decisions	Business Analyst Financial Analyst
	 Data-Driven Decision Makers	Leverage data to inform strategic and operational decisions	IT Project Manager Marketing Manager

Source: Steven Miller and Debbie Hughes, The Quant Crunch: How demand for data science skills is disrupting the job market (Burning Glass, IBM and BHEF, 2017)

Data Organisations

Big data solutions can be segmented into Infrastructure, Analytics, Applications, Data Sources, Cross Infrastructure/ Analytics, and Open Source categories. An example of the major players in the Analytics segment is shown below. ■

<p>ANALYTICS SOLUTIONS</p>	<p>DATA VISUALISATION</p>	<p>SOCIAL MEDIA</p>	<p>STATISTICAL COMPUTING</p>
<p>LOCATION / PEOPLE / EVENTS</p>	<p>ANALYTICS SERVICES</p>	<p>SENTIMENT ANALYSIS</p>	<p>IT ANALYTICS</p>
<p>BIG DATA SEARCH</p>	<p>REAL-TIME</p>	<p>CROWDSOURCED ANALYTICS</p>	<p>SMB ANALYTICS</p>

Source: Adapted from genkiware.com, *Big Data Landscape*, 22 February 2019.

The Changing Face of Digital Analytics

By **STEPHEN RAJ**, General Manager, Digital Business (Asia Pacific), UST Global



The rapid changes in data and their underlying analytical platforms have transcended from being strong value creators to becoming increasingly challenged in their relevance to the future needs of today's enterprises. What are the trends and underlying principles that will drive success in the future for enterprises?

As we accelerate deeper into the digital economy at unprecedented rates, almost every strategy around digital has, at its fundamental core: data.

What used to be created by humans at a moderate pace through careful introspection and deliberate purpose is now being almost churned out at bewildering speed by an array of technologies. There are about 2.5 quintillion bytes of data created each day (where a quintillion is 10 to the power of 18, i.e. 10^{18}), and most of that has been created in the last two years.

This mind-boggling amount of data is created through an ever-increasing range of sources that span from enterprise systems, social media activity, internet searches, image recordings, voice recordings and the plethora of sensors forming the Internet-of-Things ecosystem.

While it used to be possible for humans to be able to interpret data and make business decisions from them, it will be increasingly impossible to do that as we race faster down the speedways of the digital economy.

Autonomous decision making

Data will increasingly be subject to broad governance frameworks and authorised to autonomously participate in decision making.

Machine learning and artificial intelligence are already slowly replacing humans as the consumers of data for decision making, many of which result in physical actions. For instance, how many of us even question the validity of the directions suggested by the global positioning systems on our phones and cars?

As the world moves from analogue to digital, this requires a careful and calculated approach

to data and decision making. Businesses need to capitalise on the current practical uses of data and analytics for decision making. At the same time, we must prepare for the eventuality that we will need to control the behaviour of data-driven decision making without actually participating in the decision making (see box, “Evolution of Data”).

Types of data analytics

Before we discuss how organisations and boards can leverage data and analytics, it is imperative to understand the four types of data analytics.

1. **Prescriptive analytics** refers to analysis based on the rules and recommendations in order to prescribe a certain analytical path for the organisation.
2. **Predictive analytics** ensures that the path is predicted for the future course of action.
3. **Diagnostic analytics** is about looking into the past and determining why a certain thing happened. This usually revolves around working on a dashboard.
4. **Descriptive analytics** is based on the incoming data. The mining of the data deploys analytics that comes up with a description based on the data.

Data analytics evolution

The collection, management and exploitation of data with analytics is no longer just about ensuring survival in the present. It is increasingly also about helping to chart the future course of businesses.

The nature of data and the nature of its use is changing rapidly.

While the first generation of analytics provided a competitive advantage to many enterprises, it soon became quite useless as the volume of data and information explosion far surpassed the ability to process and capitalise on it.

While there continues to be many big data analytics implementations by enterprises hoping to get the same insights and edge as large digital companies like Google, Facebook and Amazon, many of these implementations with large investments raised hopes but did not deliver the results they had promised.

The constant evolution of analytics capabilities has resulted in many enterprises now having multiple layers and flavours of data services, such as master data management, metadata management, data

architecture, data integration, data lakes, data wrangling, etc.

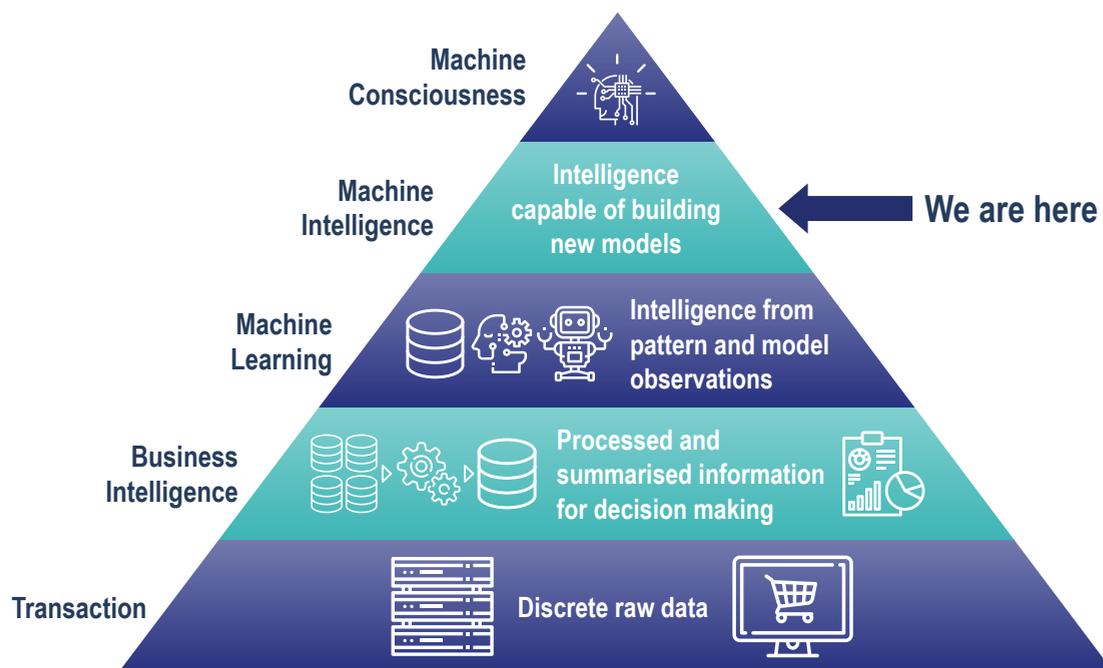
As the nature of analytics has evolved, so has the underlying technology stack. Many enterprises are now struggling with a convoluted technology stack as a result of this rapid evolution of the nature of data and analytics platforms.

What happens next

What are the trends in the data analytics evolution?

For one, successful organisations are combining data from different sources – structured and unstructured. Data, from devices and social media, is extracted and combined in a manner that provides a very rich set of inputs to make analysis meaningful.

Evolution of Data



This process combines the old and the new seamlessly so as to not only exploit data in data warehouses but also big data appliances. Data is integrated from a wide range of sources to provide views that expand the insights. This requires newer information technology, data architectures and organisations that can help the right implementation road maps evolve faster.

Newer technologies are faster and can get to insights faster than before. Agility and speed are capabilities that successful organisations master.

Successful organisations also focus on the people side of data.

The business and IT people need to work together and form cross-disciplinary teams so that analytics is no longer just in the realm of technology but is “democratised” where people in all parts of the organisation can use and avail themselves of the benefits.

These organisations have champions and sponsors at the highest levels of the enterprise like Chief Data Officers and Chief Analytics Officers so that the data-driven philosophy is communicated top-down and implemented bottom-up in the organisation.

As a consequence, these organisations go beyond descriptive analytics and reporting, to more sophisticated analytics. They use prescriptive and predictive analytics to provide insights that extend the capabilities of decision making, with just-in-time information to make quick decisions.

The survival and growth of an organisation in the future will depend on how even more dramatic changes in the world of technology

impact the creation of data and the ability to exploit that through analytics. This maturing of platforms, frameworks, tools and technologies has created a new breed of analytical capabilities that is on the horizon and is now being realised.

The advent of machine learning, artificial intelligence and robotics brings the next generation of analytics in focus where machines make decisions for us and aid decision makers in ways that we have not seen.

Future-proofing the enterprise

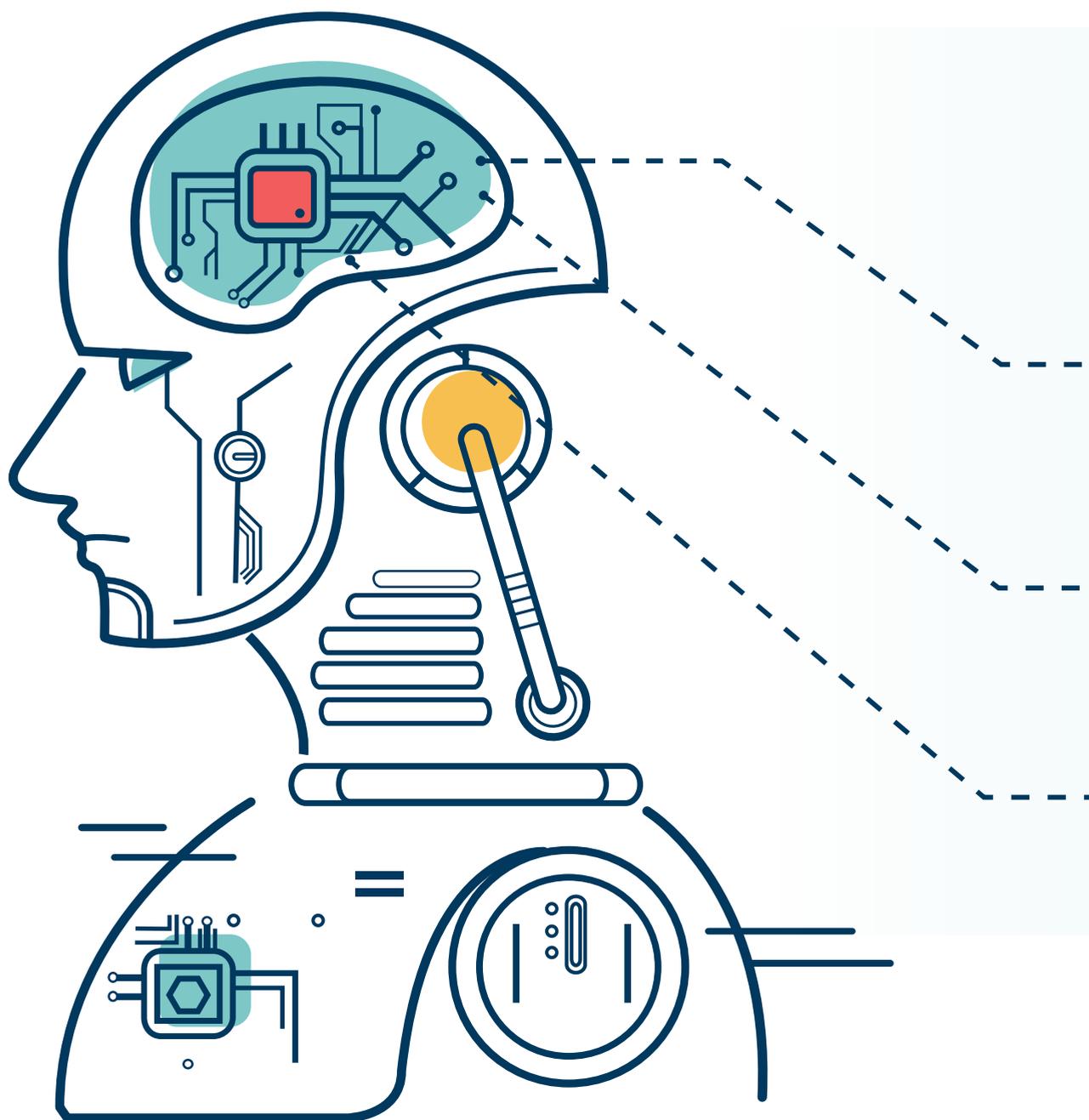
How do the board and management keep up with all these changes to ensure the survival of the enterprise in this new data age?

The answer is the ability to assess the environment and recognise the changes taking place in the world of data and information. Companies have to be able to analyse and act quickly in response to the rapid changes in data evolution.

In short, businesses must be able to:

- Assess current capabilities, maturity of processes, technologies and underlying processes.
- Innovate and incorporate new tools, technologies and frameworks to drive the analytics evolution.
- Build a data-driven organisation that bases decisions on data and facts and not just on gut instincts.
- Democratise data, create a cultural change so that all parts of the business and processes have access to data and analytics.

Thus, evolving the analytics capabilities and creating a data-driven enterprise are key to ensuring the survival and success of an enterprise. ■

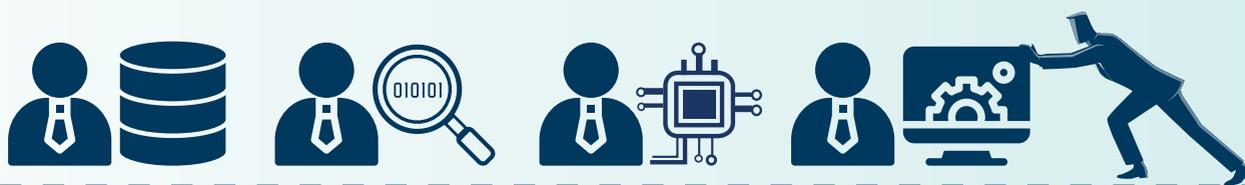
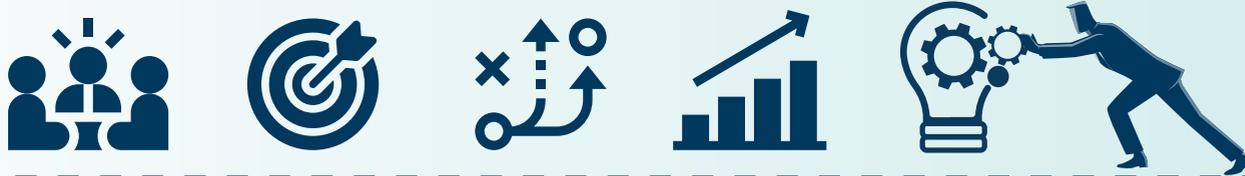


Delivering AI at Scale

By **LEE JOON SEONG**, Managing Director, ASEAN Lead, Applied Intelligence, Accenture

The majority of Singapore companies struggle to move beyond experimentation to aggressively deploy AI across their organisations. For those who successfully manage to create an organisation powered by robust AI capabilities, the rewards can be immense.

3 Steps to Scale AI



Artificial intelligence or AI is often hailed as the next digital frontier for business and industry transformation. But are businesses using it at scale or even using it?

Recent research shows that 88 per cent of Singapore executives believe they will not achieve their growth objectives without scaling artificial intelligence (AI). More startling is that 76 per cent acknowledge they risk going out of business in five years if they do nothing to change this.

The fact is that almost nine in 10 corporate leaders acknowledge that while they know how to pilot AI, they struggle to scale AI across the business.

The research found that while AI implementation is pervasive across enterprises, companies are stuck in a seemingly infinite loop of “proof of concepts”, where the company embarks on experiments on feasibility testing, but never quite implements and scales AI to realise its full potential.

These companies are unable to extract value from their data and investment in AI technologies. Contrasting these with those that managed to get it right, the “strategic scalers”, achieve nearly three times the return on investments and an average 32 per cent premium on key financial valuation metrics.

How Crucial is Scaling AI to Your Business?

GLOBAL

SINGAPORE



of executive say they won't achieve their growth objective without scaling AI.



of executive believe they risk going out of business in 5 years if they don't scale AI.



of executive acknowledge they know how to pilot, but struggle to scale AI across the business.

Source: *AI: Built to Scale – From experimental to exponential* (Accenture, November 2019)

What must companies do to close the gap? Here are three steps to start companies on the journey to strategically scale AI and get the returns.

1. Get the basics right – the data foundation.

Successful AI deployment depends on one major factor: data. This may be obvious to enable strategic scaling of AI, but the obvious is often the most ill-executed.

The rapid rise in volume, velocity and variety of data has resulted in significantly more complex cleansing, managing, maintaining and consumption of data. Companies today have more data than ever, yet they are also getting more data “noise” than useful insights.

Many still struggle with disparate data sources and data silos. They grapple with the true definition of data fields, the relevant data lineage and the composition of it. And adding more complexity to this is the need to fully comply with the Personal Data Protection Act and General Data Protection Regulation, protecting data against misuse, security breaches, and gaining consumer trust by ensuring data privacy.

After years of collecting, storing, analysing, and reconfiguring troves of information, most organisations still struggle with the sheer volume of data and how to manage it.

In an environment where data foundation is severely inadequate, even the best and greatest AI innovation borne out of a data sandbox will find it difficult to scale. A properly architected productionised environment requires data and model pipelines to be seamlessly integrated and managed to produce results in ways that are transparent, reliable and consistent.

This means going back to getting the basics right – creating a solid and robust data foundation. Simply swapping from a traditional data warehouse to a new data lake does not mean much in reducing data noise or advancing AI agenda.

Companies need to do much more than that, and this means looking at data foundation as an integrated portfolio of data capabilities that needs to be addressed holistically, systematically and often, painstakingly. And it is more than just

simply putting together the latest state-of-the-art technology stack.

For example, the traditional data governance framework needs to be redefined, incorporating new considerations especially where data is used to feed AI recommendation systems. This requires greater transparency on the types of data and rules used in decision-making process.

Data management “2.0” should be a comprehensive data management framework strategically built to enable AI at scale. It should comprise next generation capabilities in the area of data governance, data architecture, data security, data access and sharing, data privacy management and metadata management

2. Success can only happen by design.

As the development of data and analytics capabilities takes centre stage in companies’ investments, this calls for more focused leadership to drive impact. The creation of new leadership roles – namely, Chief Analytics Officer and Chief Data Officer – is just one aspect. Establishing clear C-suite ownership and sponsorship is a critical step. The organisation needs to identify who takes leadership in advocating and strategically putting the AI roadmap in place, to ensure the success of AI initiatives.

Aligning AI with business goals and scaling with intention is another factor that needs to be looked at. AI needs to be implemented not just for the sake of AI, but rather designed to solve or meet a specific business need.

Then the next set of questions are defining the “what”, “why” and “how”. For example, which functions within the organisation should receive the prioritised investment for AI? What benefits can be expected out of that investment? How do we measure the success of AI?

The “what” identifies the opportunities where AI can deliver impact while the “why” addresses the business case for change. The “how” addresses the roadmap and the operating model for AI. This requires a clear plan of action.

All these can only happen by design, with strong sponsorship from the very top.

3. Get the right talent mix – don’t forget the “artist”.

Data scientists are the critical talent every organisation needs, to successfully implement AI. The science of data, however, needs to marry with the art of analytics and AI to achieve lasting impact. The combined power of data scientists working alongside analytics/AI talent will help bridge the chasm between the science of data and the art of business.

Talent who can build business models based on compelling AI-powered stories are key determinants of the success and failure of AI implementations.

In fact, the effort of scaling calls for embedding multi-disciplinary teams throughout the organisation, teams with clear sponsorship from the top ensuring alignment with the C-suite vision. Led by the Chief AI, Data or Analytics Officer, they are ideally comprised of data scientists, business and functional analysts, data and AI engineers, UX designers, visualisation experts, change agents and other specialists. Companies looking at strategically scaling AI must put in place the right talent mix.

In closing, strategically scaling AI across the enterprise is a journey and it is by far one of the most transformational journeys to be undertaken by companies in the coming years. Strategically scaling AI creates competitive differentiations to pull away from competition. Failing to do so however can also mean the demise of great enterprises who either don’t see that coming or fail to act with speed and agility. ■

Improving Corporate Governance with Distributed Ledger Technology

By **KHOONG HOCK YUN**, Operating Partner (BlockChain Fund), Tembusu Partners



The inefficiencies and even ineffectiveness of corporate governance are largely due to the increasing distance between shareholders and companies. Distributed Ledger Technology, as a peer-to-peer trust protocol that removes the need for some or all intermediaries, offers a great opportunity for better corporate governance.



Blockchain has taken the world by storm.

In a way, its origin came about from the repeated financial scandals such as the collapse of Enron (2001), WorldCom (2002) and Lehman Brothers (2008). At the height of the global financial crisis in 2008, and with growing distrust of the financial establishment, a person or persons going by the pseudonym of Satoshi Nakamoto introduced the concept of blockchain to track ownership of an electronic currency called the “Bitcoin”.

Since the advent of the bitcoin, some other 800 cryptocurrencies have been created. Beyond

cryptocurrencies, there have been initiatives to apply blockchain technology in other industries and application areas.

However, blockchain is, in essence, a form of Distributed Ledger Technology or DLT (See box, “Blockchain vs DLT”).

Trust

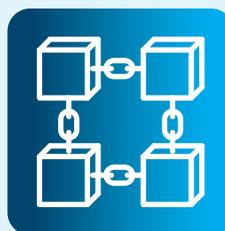
The main reason for the interest and take up of DLT is that it enables trust in peer-to-peer transactions, without the need for intermediaries.

While the internet enables rapid business growth

Blockchain vs DLT



A distributed ledger is a decentralised database, distributed across several computers or nodes. Every node maintains the ledger. If any data changes, the ledger is updated independently at each node.



A blockchain is one form of DLT where every node gets its own copy of the ledger. When a new transaction is added, all copies of the ledger get updated.

In a sense, DLT is the parent technology of blockchain, and blockchain is one of the most advanced versions of DLT.

The main differences:



Block structure

Blockchain represents the data as a chain of blocks. Data can be represented in different ways in distributed ledgers (not just in blocks).



Sequence

All blocks are in a particular sequence. DLT uses different sequences of data depending upon the technology.



Power Hungry Consensus

Typically, there is a wide usage of proof of work mechanism in the blockchain, which take up power. DLT does not necessarily need this kind of consensus, so it is comparatively more scalable.



Tokens

Distributed ledger economy does not require tokens or any kind of currency on the network. Blockchain platforms traditionally have some sort of token economy, although newer implementations are trying to change that.



Implementations

Many enterprises and governments are already using blockchain technology. DLT projects are still under development.

through global connectivity, empowering strangers to easily conduct business with one another, trust has to rest in the hands of third-party intermediaries to confirm the veracity of digital dealings made between two parties.

With the financial scandals, trust in companies, intermediaries and regulators is being questioned. Can corporate executives be trusted to always deliver on their promises?

DLT grew out of this concern over corporate governance. It does away with the need for intermediaries to validate and verify the transaction.

DLT employs cryptography to secure data. It uses consensus algorithms for the community to verify the validity and to authorise the addition of new transaction records to previous records in a chain of blocks of transactions (the Blockchain). See box, “How DLT Ensures Data Integrity”.

In a DLT world, the role of a verifier is decentralised to all network participants, removing the need for the existence of a trusted intermediary to make things work.

For example, to add a bitcoin transaction, powerful computers in the network (called “miners”) compete to be the first to solve a cryptographic puzzle that enables them to verify and secure the new transaction. Winners are awarded bitcoins, which are collected as transaction fees from the user who initiated the transaction. This consensus algorithm is called “Proof of Work”. There are many other types of consensus algorithms.

When a block is confirmed in a blockchain, the data in any given block cannot be altered retroactively without modifying all previous blocks. Changes would require the consensus of the network – making blockchain secure by design. Data is also harder to manipulate or attack as different nodes in the network hold these records.

Smart contracts

As blockchains can store data, it can similarly store and execute computer applications accessible in a decentralised manner across the world. In 2013, Vitalik Buterin, a cryptocurrency researcher and programmer, proposed Ethereum, which is both a cryptocurrency and a decentralised computing platform.

This led to the rise of smart contracts, agreements between parties in the form of business logic or computer programmes. They automatically execute when certain conditions are met (e.g. pay dividends when certain share price targets are achieved).

Smart contracts use digital signatures to verify participation and assent to agreed terms.

Governance failures

Many of the financial scandals are the result of failures in corporate governance.

Fundamentally, owners of companies have the right to control the company and receive its earnings. In corporate law, most of the key decisions are being made by a board of directors.

But the interests of shareholders and those of board members can diverge, even conflict. Adam Smith referred to this as the “agency problem”. For example, board members may be there and make decisions for the power, prestige and money bestowed on them, and sometimes at the expense of minority shareholders.

Corporate governance focuses on the question of motivation of corporate board members to act in the interests of their stakeholders. and formulates contractual and regulatory solutions. But these solutions are generally costly and over time, have not been fully effective. When there is a corporate governance failure, shareholders are usually the ones most severely impacted.

With its “trust protocol”, DLT can offer smart solutions for classical inefficiencies in the corporate

How DLT Ensures Data Integrity

Hash functions are used in DLT to ensure data integrity of digital signatures and Message Authentication Codes (MACs).

A hash function is a mathematical function that converts a numerical input value into another compressed numerical value. The input value is of arbitrary length but the output (known as the “hash value”) is always of a fixed length (typically, 128 to 512 bits). Popular hashing algorithms include RSA, Whirlpool, MD Algorithm, SHA and RIPEMD. The key properties of hash functions are:

- **Pre-image resistance.** If a hash function $h(x) = y$, y cannot be reverse computed to x .
- **Collision resistance.** Two different input messages should not hash to the same output i.e. $h(x) \neq h(z)$ when $x \neq z$ (where \neq means “is not equal to”)

Message integrity and authentication are upheld with the possession of a Private Key (that you hold yourself) and a Public Key (for everybody to use) to enable encryption and decryption. Schematics on how it works are shown below.

Application 1: Cryptography used in sending Private Messages



Application 2: Cryptography used in sending “Signed” Messages



governance field. Some of these DLT solutions are in various stages of implementation around the world.

Greater transparency of ownership

The Delaware Blockchain Initiative and Daura AG are examples of efforts to list company shares on a public blockchain. In effect, we will have real-time accurate records of stock ownership. Such records are only readable by the right people, provide confirmation of who sent them, and provide confirmation that they have the assets to be traded.

Using DLT for share registers reduces opportunities for arbitrage and fraud.

But some shareholders may not be attracted to this arrangement. Activists, raiders or managers might wish to conceal their trades for exactly the same reasons that minority shareholders, retail investors and fund managers might wish to see them.

On the other hand, issuing companies may find public blockchains valuable to remove the secrecy prized by shareholder activists and corporate raiders when they are building hostile shareholding positions.

Access to governing documents

Shareholders need timely, relevant and complete information to monitor their share performance and to decide on the resolutions to propose or pass at shareholders' meetings in order to safeguard their interests.

DLT can enable secure, timely, and reliable controlled distribution of sensitive and time-critical information. It can also automate the workflows through smart contracts and use of corporate's private key to encrypt documents.

Symbiont is already helping Vanguard, one of world's largest investment companies, to move index data between index providers and market participants.

If shareholders and regulators could review corporate documents by logging into a DLT-enabled database, perhaps there may be fewer corporate violations and bypassing of regulations.

Fair shareholder meetings

Current problems with elections at shareholder meetings include inaccurate or incomplete voter lists, incomplete distribution of ballots, and chaotic vote tabulation.

The Estonian stock exchange began in 2016 to conduct shareholder voting on a blockchain platform. In a blockchain election, eligible voters would receive tokens (sometimes called "votecoins") that they could transmit to addresses on the blockchain to register their preferences.

Blockchain technology allows votes to be quickly and securely recorded. It streamlines the proxy voting process that has historically been labour-intensive and fragmented. Thus, it will or at least will be seen to enable and encourage the active participation of shareholders in corporate governance.

Real-time accounting

Many corporate scandals arise directly from wilful accounting malpractices. DLT in accounting could be the next big step in accounting, after the introduction of the double-entry bookkeeping system.

Blockchain accounting systems will reduce the need for traditional manual audits. It will require audit firms to redefine their roles.

The trust thrust

In summary, DLT is more than an alternative to classic ownership ledgers using double-entry bookkeeping.

The technology enables trust in peer-to-peer transactions, bypassing intermediaries. As more applications in corporate governance and beyond use DLT, it will help business be more efficient and reduce the number and cost of corporate scandals. ■

Can Pofma Protect Businesses?

By **ADRIAN TAN**

Head of Media and Intellectual Property Law, TSMP Law Corporation



Pofma is the Singapore government's weapon to stop fake news. Much of the debate has been around freedom of expression and access to information. But how effective is the new law in protecting business interests?

The Protection from Online Falsehoods and Manipulation Act (commonly known as “Pofma”) came into force in October 2019. Essentially, it prohibits people from communicating false statements of fact to anyone in Singapore through the internet or messaging services, whether via text or multimedia.

What is covered under Pofma?

A false statement of fact is defined as a untrue or misleading statement which a reasonable person would consider to be a representation of fact.

A person must not communicate anything which that person knows or has reason to believe is false.

But that in itself is not enough to trigger Pofma. Pofma also requires the false statement to be likely to cause harm, including:

- Harm to Singapore’s security, public health, public safety, public tranquillity or public finances, or its relations with other countries.
- Influence an election or referendum.
- Incite bad feelings between different groups of persons.
- Diminish public confidence in the government.

On conviction, an individual can be fined up to S\$50,000 (S\$500,000 for non-individuals) or jailed up to five years.

What makes Pofma special?

If an individual spreads fake news, and the fake news causes harm to society, the individual can be fined or imprisoned. Other countries have introduced laws against fake news, and legislated ways to punish the wrongdoer. But how can punishing the wrongdoer (if the wrongdoer can be found) stop the spread of fake news?

Singapore’s Pofma is unique among fake news laws because of certain innovations.

Let’s say a person makes a false statement which causes harm. Apart from punishing that person, Pofma also empowers the government to issue specific directions to help stop the spread of that false statement (see box, “Pofma Directions 3 and 4”).

In short, Pofma is special because it does not just provide for ways to punish people who spread fake news. It also provides for ways to block the fake news, and to point people towards the truth. That is the innovation, and that is how it can be used to help businesses – perhaps.

Is Pofma effective?

So far, much of the conversation around Pofma has centred on free speech. Since it was enacted, the government has had to rebut international media articles which alleged the use of Pofma in curbing free speech. Among the most controversial was the initial correction notice that the government issued requiring Facebook to put a correction next to a particular article. Facebook did so with a notice that “Facebook is legally required to tell you that the Singapore government says this post has false information” and expressed hope that the implementation of Pofma will not impact free expression.

The international media argued that Pofma restricts debate. The government remains steadfast in maintaining that it did not ban or suppress any information. The original posts on Facebook remains for all to see. Readers are able to read them together with the government’s response, and decide for themselves which tells the truth.

Pofma is not just about free speech, debate or politics. At its core, Pofma is about the communication of information. And when it

Case Study #1 – Tainted Infant Formula

Ms X posted on an online forum for new mothers that she used to work at Company Q, which produced infant formula. She alleged that all infant formula (not just from Company Q) are treated with chemicals that would improve taste. Unfortunately, those same chemicals are carcinogenic and pose serious health risks. Ms X said that she knew all this because she used to work at Company Q's factory, and was in charge of producing infant formula. She warned new mothers to avoid giving any sort of infant formula to their newborns, and instead rely solely on breast milk.

This post caused a huge stir among worried mothers. Some of them even wanted to organise a group to protest at Company Q's premises and demand to know the truth. Company Q knew that the post was fake news. Forensic investigators located Ms X and identified her. Ms X had never worked at Company Q. In fact, she had never

worked at all, as she had severe mental health issues. She had made everything up.

Company Q asked the online forum to delete all her posts. The online forum did nothing. Until today, mothers continue to be worried whenever they read Ms X's posts. Because it is so widely read, it still appears frequently in search results.

This case happened a long time ago, before Pofma. Can Pofma be applied?

Arguably, yes.

If the post contains false statements of fact, and causes a health scare, or disrupts public tranquillity, then perhaps Company Q can ask the government to invoke Pofma to direct the online forum to delete Ms X's post, or to require the online forum to post a correction to state the truth.

Case Study #2 – The Defective Necklace

Mr Y posted on an online forum, describing how he had bought an expensive necklace from Company A as an anniversary gift for his spouse.

Unfortunately, the necklace was defective. According to Mr Y, all the pearls and diamonds on the necklace became dislodged after the first few weeks of wear, and were lost.

When Mr Y complained to Company A, Company A brushed him off and disclaimed responsibility. Mr Y ended his post by telling readers not to buy Company A products. The post had a negative impact on Company A's review ratings.

Company A knew that the incident never happened. It carried out a forensic investigation,

and found out that Mr Y was in fact an employee working at a competitor company. Company A took legal action against Mr Y, who paid money to Company A as compensation. But the online forum continued to carry Mr Y's post, even though Mr Y wrote to the forum to ask them to delete it.

Can Company A ask the government to use Pofma?

Arguably, no.

Although Mr Y's post was fake news, it did not cause any harm to society, nor to Singapore. It caused harm only to Company A.

Directions Under Pofma

When the government deems that a falsehood has been communicated, it can issue directions under Part 3 and Part 4 of Pofma.

Part 3 Directions

Part 3 Directions are for parties who communicated the false statement.

A Part 3 Direction works in two ways:

- A Correction Direction is issued when the government directs the person to put up a notice (online or in hard copy) saying that what was communicated was false, and it may also include a correction.
- A Stop Communication Direction is when the government directs the person to take steps to ensure that the false statement is no longer available online.

Part 4 Directions

Part 4 Directions are for internet intermediaries such as companies that provide internet access (e.g. Singtel), searches (e.g. Google), social media (e.g. Facebook), messaging (e.g. WhatsApp), or video sharing (e.g. YouTube), and providers of mass media services such as a broadcaster (e.g. CNA), newspaper (e.g. The Straits Times) or online site (e.g. Yahoo News).

A Part 4 Direction can be:

- A Targeted Correction Direction issued to internet intermediaries to communicate a correction notice to all end-users who accessed such statement via that service.
- A Disabling Direction is issued to an internet service provider to block end-user access to that false statement, say on a web page in Singapore.
- A General Correction Direction is issued to a newspaper, broadcaster, telecommunication or internet service provider to tell its audience about a correction to the false statement.

comes to business, communication is a key battleground for competitors.

Unscrupulous companies, for instance, may spread fake news in order to harm their rivals, and steal their customers. Information, and its dissemination, become critical.

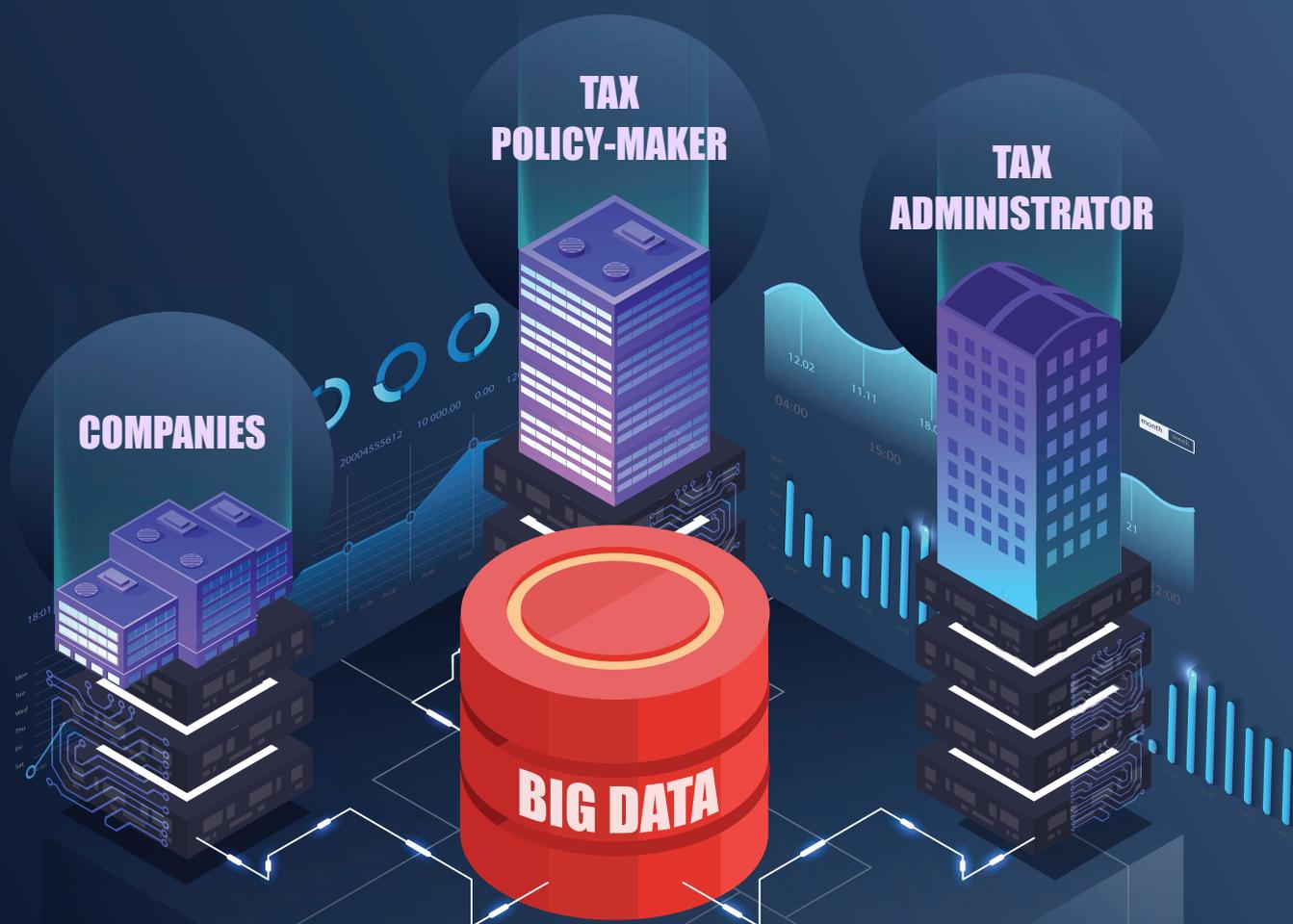
To illustrate, here are two hypothetical case examples (see box, “Case study #1” and “Case study #2”). They are adapted from real-life cases, but the identities and products have been changed, for reasons of confidentiality.

From the case examples, it would seem that Pofma has its limitations when applied to business. If a competitor spreads fake news about a business, the company can sue the competitor for compensation, but the fake news may continue to remain on the internet.

It is possible to use Pofma to remove or correct the fake news, but only if the government can be convinced that the fake news in question is harmful to Singapore or to society. It all depends on how one looks at fake news, and its wider implications. ■

Taxation in the Global Spider's Web of Big Data

By CHUNG-SIM SIEW MOON



Big data is having a profound impact on taxpayers, tax policy-makers and tax administrators around the world. What should companies do, to ensure that they are adequately prepared for the transformational changes that are occurring to both the policy and administration of tax?

Globalisation, technology and digitalisation are transforming the world. Specifically, the existence and exploration of big data marks an important step in our ongoing quest to quantify and understand the world in a more meaningful, holistic and value-adding way.

Big data allows us to do more. With added data, we can see and understand the relationships between different pieces of information. Until a decade or so ago, we could guess at, but never fully grasp, the messages hidden in the terabytes of data that we now have access to.

Today, the power of big data is a game changer. The speed of data creation is unrelenting – but equally important is the ability to analyse data, act on it and draw value from it.

How does your company stack up in its ability to harness these changes? And what more can you do as a director to ensure that value from data is captured and risks managed?

Impact on tax

The tax community is a particularly active participant in the rapid rise of big data, which impacts companies, tax policy-makers and tax administrators alike. Each wants to extract as much value as possible from big data, while simultaneously protecting their interests from other members of the tax community. What exactly is big data from a tax perspective?

Simply put, data is the lifeblood of tax.

Tax is a numbers game and the volume of data for those working in tax is staggering. Think of those from electronic invoices, sitting within general ledger accounts, value-added tax (VAT) and goods and services tax (GST) transactional data in virtually every country, from point-of-sale systems and other accounting tools, etc. The list is endless.

There is also data that companies must present to tax authorities, often in real-time or very close to it. This includes the so-called standard audit files for tax purposes (“SAF-T”) that many European nations require, and VAT or GST information that must be submitted, often monthly or quarterly.

Additionally, multinational enterprises must now also submit files called country-by-country reports which contain a range of tax and financial information. These must be submitted in more than 80 jurisdictions each year, each with its own domestic digital tax data submission requirements. The European Union, meanwhile, has introduced new disclosure rules aimed at increasing transparency and detecting potentially aggressive cross-border tax planning.

This web of information is then exchanged, spontaneously and automatically, between countries under new information exchange rules. As a result, any data submitted in Country A can be expected to be available in Countries B through Z very shortly thereafter.

So the volume of big data is increasing. But why is it so important in tax?

Companies

For businesses, the importance of big data lies in two areas.

The first involves opportunities to wrangle, arrange and query big data, creating top- and bottom-line opportunities. These include, among others, the opportunity to reduce customs or excise costs; identifying timing opportunities, and using machine learning, robotic process automation, artificial intelligence and the like to analyse and leverage big data more astutely.

The second area is risk mitigation. This includes running the same tests as the tax authorities are likely to run, but in advance of filing a tax return

or digital data submission. This can help to reduce the volume of incoming enquiries, leaving scarce tax resources available for more value-adding activities.

Tax policy-makers

For policy-makers, big data presents a unique challenge. As the European Commission noted in 2018, “value is often created from a combination of algorithms, user data, sales functions and knowledge. For example, a user contributes to value creation by sharing his/her preferences (e.g. liking a page) on a social media forum. This data will later be used and monetised for targeted advertising”.

This notion of user data value sits at the heart of what could potentially end up being the most significant changes to the international tax architecture for more than a century, with the Organisation for Economic Co-operation and Development (OECD) trying to secure consensus on new tax rules amongst more than 130 jurisdictions.

Meanwhile, user data value is also driving a number of jurisdictions to put in place “interim” digital services taxes while a long-term solution is debated.

Tax administrators

Big data is equally important to the taxing authorities. Here, all the incoming data from businesses outlined above are mingled together, allowing complex data analytics routines and voluminous data-matching to take place. These routines provide tax authorities with both insights (looking at past trends, organising and mining the data) and foresight (predictive analytics).

Tax authorities gain more insights into the taxation patterns and behaviours of their own jurisdiction and globally, helping their enforcement, collection of taxes, and tax audits as well as helping tax policy-makers deliver the best policies.

Another big data initiative is the *Analytical Database on Individual Multinationals and Affiliates* released by the OECD in July 2019. This database provides a world view of about 100 of the largest (by sales) publicly traded (and not state-owned) multinational enterprises (MNEs) globally. It includes where they are located, how they operate, and where they pay taxes. Several open big data sources were used to collect information on individual MNEs and their global footprint.

On home ground, the Inland Revenue Authority of Singapore (IRAS) is prioritising using data intelligently and embedding analytics in its processes and systems. IRAS uses advanced statistical techniques to sift through its information repository to derive new understanding from existing data and predict future trends, identifying businesses with higher non-compliance risks and to detect non-compliance and evasion.

This is especially apparent with more probing and complex controversies being observed, and more audits and higher publicity of tax crimes. The results are solid. For example, IRAS recovered S\$175 million in GST and related penalties from audits and investigations during the first nine months of 2019.

Why should taxpayers pay attention?

Some countries embracing digitalisation now require the bulk of company data submissions to be made digitally. With technology, it would not be difficult for such tax authorities to generate notices to taxpayers who fail to meet the deadlines for digital submission requirements and impose penalties.

Brazil is a good case in point. If a company chalks up too many “digital infringements”, it may find itself at operational risk as it becomes overwhelmed and spends more time putting out fires. Companies may also face financial penalties in these cases, too. And although the financial

Checklist for Companies



1. What is the company's overall digital strategy?
 - a. From a tax governance and planning perspective.
 - b. From a tax compliance and tax administration perspective.
2. How is management monitoring global changes to tax submission requirements and preparing for new mandates?
3. Is the business' approach to digital and technology keeping pace with that of the tax authorities?
4. How do we work together internally to manage our response to tax authorities?
 - a. Do we have the resources and skills?
 - b. Do we have the tools and technology?
5. Do we have visibility and understanding of what the tax authorities are doing with our company's data?
6. Can we replicate the tests that key tax authorities are running?
7. Have we adequately prepared our tax and finance teams for digital audit defence activities?
8. Do the Tax, Finance and IT departments work seamlessly together to get the job done?

penalty may be relatively low, the costs rapidly escalate when multiplied by several hundreds or even thousands of infringements.

In cases where the data submission required is housed in systems that are dispersed around the world, in different technologies and behind different firewalls, the information technology, finance and tax departments need to come together to ensure that such routine requests can be met. But no chief information officer likes to find that the organisation's scarce resources are suddenly pulled off a revenue-generating project to meet the needs of a far-flung tax administration.

How boards can help

With the increasing role played by big data, directors are uniquely placed to ensure their

companies are adequately prepared (see box, "Checklist for Companies").

The impact of big data is keenly felt across the tax communities – taxpayers, tax policy-makers and tax administrators alike. Tax policy-makers and tax administrators are ramping up the use of big data in the areas of tax policy, tax reforms, enforcement and assessments, and it is crucial that taxpayers do not fall behind.

Taxpayers should ensure that the right baseline approach is in place now, rather than later. Support from the board is key to steering companies in the right direction. ■

Chung-Sim Siew Moon is the Asia-Pacific Tax Policy and Controversy Leader for EY. The views reflected in this article are her views and do not necessarily reflect the views of the global EY organisation or its member firms.

The Accountant and Big Data



By **GERARD TAN**
Former SID Council Member

The accounting profession has traditionally been linked to bean counting, or data crunching. In this age of “Big Data”, can the accountant survive if he continues to be good only at counting beans?

In the 2016 action thriller movie “The Accountant”, a Certified Public Accountant uncooks the books of criminal and terrorist organisations around the world. His uncanny ability to digest, crunch and analyse huge volumes of data and unravel the complex web of embezzled funds must have pulled a cord in accountants – well, it did for me.

But let’s face it, even though the movie was made not so long ago, the accounting profession it depicted harked back to the pre-internet age. That’s when numbers and accounting (read: financial data) were at the heart and bloodstream of all business. And the accountant was king. Because only we understand how to create and interpret that financial data.

Is it still the case today?

Well, the world has moved on. There are two key trends that accountants need to watch out for.

Data tsunami

First, is the explosion of data.

We no longer talk in terms of MB, but GB and TB. No, that’s not correct. Many have moved on to PB. Tomorrow, it will be EB and ZB. Even YB. Each xB being a 1,000 times that of the previous level.



COUNTING BEANS

The data tsunami is coming from the digitalisation of just about everything. From business transactions to personal data and medical records. From images to video, and even emotions.

Social media apps, such as Twitter, WhatsApp, Facebook, Instagram and LinkedIn, capture not just messages and photos, but also users’ thoughts, likes and dislikes, political inclinations, consumer habits and social networks.

And the important thing is that most of these data are non-financial in nature. They no longer are in our domain – unless we ensure they stay in our domain.

Harnessing data

The second trend is that a plethora of tools have emerged to exploit the wealth of data. They go by generic names like data management, data analytics, data mining, machine learning, predictive analytics.

They essentially allow for big data to be recorded, stored, processed in a structured, secured manner. They bring data to life.

And the people using these tools are mostly non-accountants.

For example, marketing people use consumer and social media data to understand fashion and taste changes to plan their future product line-up and marketing campaign.

Data governance managers, especially in financial institutions embed algorithms in computer systems

to automatically trap unusual transactions, uncover fraud, identify regulatory breaches and unauthorised activities such as money laundering.

Human resource professionals are using personnel data to profile, measure, analyse and even predict the behaviour of employees.

Logistics personnel use data collected as goods move through the supply chain to track shipments, identify bottlenecks and support just-in-time procurements.

The list can go on.

Accountant's role

What is the accountant to do in this brave new world of big data?

We should embrace it and play a leading role in the organisation's use of big data.

To start, we can leverage on the data tools and information resources to support and enhance the value of our financial reporting and management reporting. The accountant can acquire the skills of a data scientist to use data analytics to obtain more timely and greater insights from the financial data. This could help perform continuous and timely risk monitoring and compliance checks.

More than the accounting and finance function, the accountant can show the way for the other parts of the organisation.

Most of the data generated needs to eventually reside in the company's computer system and find its way into data warehouses to be useful. Data warehouses were traditionally the preserve of the finance and accounting function.

So, it's a matter of the finance function to expand the data warehouse platforms to accommodate the new forms of non-financial data as well.



Then it should provide and support the other organisational units and users with the tools to harness the data.

Sustainability has emerged as a key need in organisations, especially listed companies where sustainability reporting is mandated. Much of sustainability reporting refers to non-financial information.

As it is new, there is no industry-wide practice as to where sustainability reporting is parked in the organisation. Again, this is where the finance function can take the lead to produce sustainable reports in tandem with the annual report.

The importance of non-financial information is recognised by auditors. Since 2017, the enhanced audit report requires that the auditor also reviews the annual report (which contains primarily non-financial information) and comments on the consistency of these "other information" with the financial statements.

Time to step up

The accountant of the future can no longer be a pure number cruncher of historical financial data. He (or she) needs to acquire the knowledge and skills of a data scientist, combined with the training and curiosity of a financial sleuth, to discover trends and patterns in the world of big data.

And he should do it for the whole organisation, and be much appreciated for it. ■



Managing Data Risks with Internal Audit Support

By **NICODEMUS TAN**, Governor, The Institute of Internal Auditors Singapore

Managing data risks is becoming more critical with the wave of new technologies. The internal audit function should provide enough assurance on data risk management by reviewing the framework holistically and the lesser known risks in depth.

Computers have become entrenched in our everyday lives, and global interconnectivity has forever changed how we work. The Internet of Things, fifth generation networks and other exponential technologies have increased the pace of change. Many companies have embarked on digitalisation with different levels of maturity and success.

The myriad kaleidoscope of technologies, legislations and human interfaces pose an array of risks that is unprecedented. In this environment, the lack of an active risk management framework can spell business failure.

Types of data risks

Well-known risks such as data corruption or data compliance risks have been widely discussed. While a plethora of countermeasures may have been developed and adopted, businesses should be prepared to keep pace with the changes that are continually needed.

Even countermeasures to familiar risks such as data loss from hardware failures, human errors, server room mishaps or malicious attacks by hackers, are not as straightforward as one may imagine them to be. For instance, while it is intuitive to perform backups, the frequency (e.g. continuous, hourly, daily), type (e.g. full, incremental) and location (e.g. local, offsite, cloud) carry different costs and benefits.

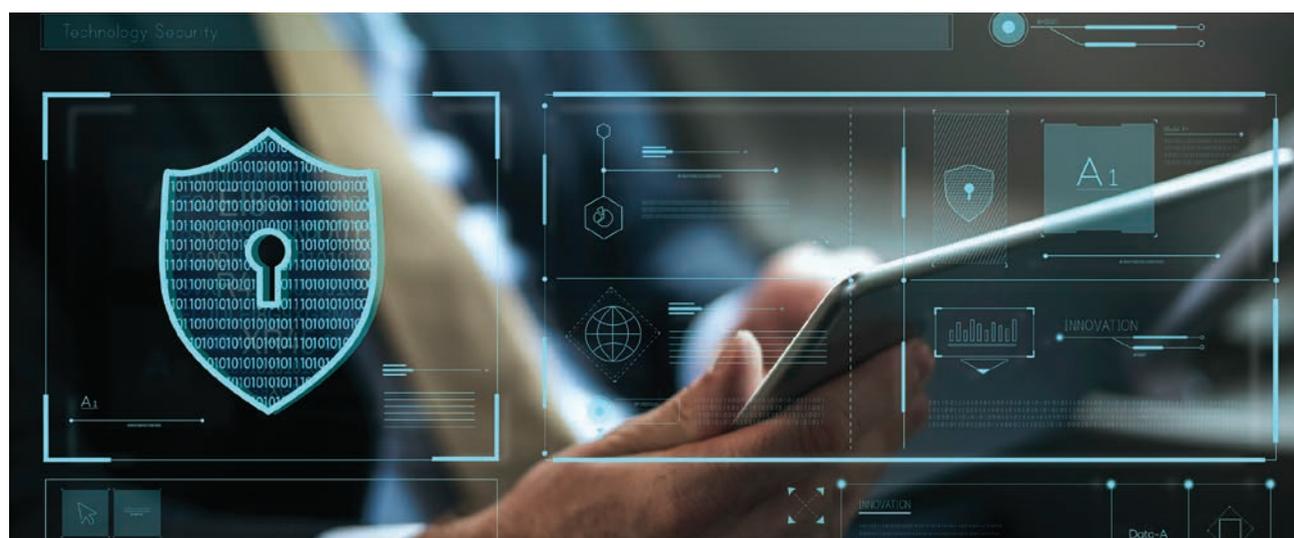
Care must be taken to select the most appropriate solution for the company, as there is no one-size-fits-all framework.

There are also lesser known or thought about data risks such as vendor lock-ins. These occur when vendors severely limit the company's ability to access or transfer data upon changing vendors. This is not just limited to information technology-related vendors but may also arise from trading platforms used for purchases or sales, or employee portals which are housed externally.

A good prevention strategy is to work only with reputable vendors within a trusted jurisdiction. All vendor contracts and service-level agreements should be reviewed thoroughly for specified timely and unfettered access to data and rights to compensation for delays. An alternative is to host key data internally and/or obtain periodic backups from the vendors.

Another lesser known risk is that of data remanence. This relates to residual data that remains in the system even after deletion and scrubbing. Often unknown to the company, most systems do not delete a file immediately upon instruction but simply park the data at a holding area in the event that the user wishes to undo an erroneous deletion. Most file systems only remove the file names from the active directory when one hits the "empty recycle bin" button. The files still reside in the allocated space which may never be overwritten by newer files, given the vast size and low cost of memory these days.

Techniques such as over-writing or degaussing may clear data residing within the company's control but may not eliminate data remanence in cloud computing or third-party backup systems. Adequate



data encryption in using cloud computing or third-party information technology resources will go a long way in mitigating such risks.

Yet other lesser known risk is that of “dark” data. This refers to data which the company has collected but did not use. Over time, dark data consumes unnecessary resources, slows down processing and leaves the company vulnerable to possible security, storage and compliance issues.

The key to managing dark data is a periodic assessment of data usefulness. With advanced data mining techniques, especially in terms of association and clustering, value may be gleaned from dark data to achieve improved sales or customer services. Where the data is not deemed useful, it should be deleted, and appropriate safeguards taken.

Risk management framework

A good data risk management framework is essential to keeping data risks within acceptable parameters. Most companies start by mapping data and formally establishing a data risk management policy that is endorsed by the board of directors.

The key steps include:

- **Create an inventory.** List the types of data being captured, points of capture, how it is

captured, where it is housed and what it is used for.

- **Identify the risks.** Classify what are the risk events that may occur, and what are the legal and regulatory requirements applicable to the data.
- **Analyse the risks.** Evaluate how frequently the risk event will occur and what is the damage when it occurs.
- **Treat the risks.** Select suitable cost beneficial countermeasures and assess if residual risk is within acceptable levels.
- **Monitor and review the risks.** Appoint risk owner(s) who will be responsible for monitoring key risk indicators and updating the data risk register on material changes or breaches in risk management.
- **Perform reviews periodically.** Review the implementation of data risk management continually and the framework annually.

In reviewing the data management framework and its implementation, the board needs to ask the right questions. (See box, “How prepared is the company against data risks?”).

Role of internal audit

Many internal auditors have sought to respond to the surge in emerging technologies. They have acquired and developed expertise in reviewing disaster recovery procedures and business

How prepared is the company against data risks?

- Does the company have an inventory of its data?
- Is there a formalised data management or data risk management framework in the company? Are the relevant staff trained and familiar with the framework?
- Does the company's risk register feature data risks? If yes, does it include lesser known data risks?
- Are the CEO and/or CFO familiar with the data architecture, risks and controls of the company? What is their stand on mitigating data risks?
- Is data management a standing item in key management meetings?
- When is the last time the company tested its disaster recovery procedures or business continuity backup plans? Are there any key system(s) with an unacceptable recovery time actual?
- Has the internal audit team performed a review of the data management framework? What is its assessment of the residual data risk?

continuity plans. However, most of them only review data as part of disparate processes and focus mainly on data accuracy and data integrity.

A good internal audit function can and should provide more assurance than that.

It should be auditing the data management framework holistically in accordance with standards such as the International Professional Practices Framework promulgated by The Institute of Internal Auditors.

It should seek to review controls over lesser known risks in its process audits. For example, the internal auditor should consider vendor lock-in risks when evaluating vendor contracts or consider the permanent removal of data in reviewing hardware management.

The internal audit team should also conduct a review of data security that goes beyond rudimentary reviews of access rights and

data backup controls. It should consider, at a minimum, the cyber security framework, phishing awareness programmes, training programmes for employees, and the timely patching of software.

At the next level, the internal audit team should also actively perform analytics of the company's data to identify trends and patterns essential to understanding and managing risks. These could include assessment of relevancy of data maintained (e.g. number of times certain data was accessed in a period) to identify dark data or compute the total value lost at recovery time actual vs recovery time objective.

Most companies have embarked on an arduous but necessary data journey and are familiar with common data risks. However, data risks and countermeasures are constantly and rapidly evolving, and a robust data risk management framework supported by an effective internal audit function is paramount to avoiding costly pitfalls. ■

Burgeoning Demand for Data Centres in Asia Pacific

By **TOM DUNCAN**

CBRE Executive Director, Data Center Solutions, APAC



Data and data centres form the backbone of technology-driven societies. As enterprises increasingly search for outsourced solutions to their data storage and processing needs, investors are deploying capital into the data centre sector.

The world is consuming data at an exponential rate. The rapid growth of the Internet of Things, fifth generation networks, and machine-to-machine communication is pushing data usage to new heights.

In 2019, there were over 4.4 billion active internet users. While internet penetration in the US and Europe stands at 90 per cent, it is only between 50 and 60 per cent in the Asia Pacific. Unprecedented levels of population growth, urbanisation and smartphone access in the Asia Pacific will fuel greater levels of data growth and demand for data centres.

With latency bandwidth restrictions and data sovereignty laws often requiring data to be processed geographically close to where it is consumed, demand for data centre facilities in urban areas is at an all-time high. This in turn has led to global pressure for supply to keep up with demand.

Right data centre strategy

From an enterprise perspective, figuring out the right data centre strategy for the business is critical to the success of the overall information

technology (IT) strategy. Many companies are re-assessing their IT strategies to adapt to the challenge of constantly evolving technologies. There is however no one-size-fits-all solution.

A common issue that businesses grapple with is uncoordinated procurement due to regional growth and mergers and acquisitions. There may also be significant pressure to ensure that IT equipment is fit for purpose and being procured at best value via an auditable process.

Currently, the majority of enterprises still store data and run their servers on their own premises, or on-site. This requires significant capital investment, bearing in mind that the replacement cycle is 10 to 15 years, while the lifespan for servers is usually two to three years.

Another potential issue is the risk of redundancy, and whether businesses can invest the necessary capital expenditure to keep pace with changing technology. Enterprises should also consider the fact that it may not be commercially viable for them to build their own facility, especially when there are other options available in the market.

Outsourcing

As a result, companies are increasingly turning to outsourcing as a more cost-effective option. There are two main models to choose from.

The first is co-location, which involves housing the company's IT equipment in data centre facilities managed by third party specialist operators. Data centre co-location facilities provide space, power, cooling and physical security for the server, storage and networking equipment of firms, connecting them to telecommunications and network service providers.

Co-location offers a few key benefits, such as the flexibility to increase or decrease capacity according to the company's real estate strategy. Another advantage of outsourcing to a dedicated facility is that it guarantees that the necessary operational, technical and security standards will be met.

The second outsourcing model relies on cloud hosting services. Cloud hosting is the process of outsourcing an organisation's computing and storage resources to a service provider that offers its infrastructure services in a utility model. Unlike traditional hosting, solutions are not deployed on a single server. Instead, a network of connected virtual and physical cloud servers hosts the application or website, ensuring greater flexibility and scalability.

While cloud computing has emerged as a major trend in the data centre industry, that does not automatically make it the best solution for all companies. For instance, cloud services might bring greater flexibility and cost savings, but issues of data security and sovereignty should also be factored in.

It is essential for companies to understand the data sovereignty regulations in their particular market, since this will necessarily inform their

wider data centre strategy. For instance, Indonesia's law on data localisation requires electronic system providers that provide public services to have data centres and disaster recovery centres based in Indonesia as part of their business continuity plan.

When it comes to data management, there is no magic bullet. This is why more enterprises are adopting hybrid IT solutions that strike a balance between cost and security. For example, a company could choose to still house highly sensitive applications on-premise or using a reliable co-location provider, while opting for a public cloud solution for the storage demands of day-to-day business.

Flexibility is key

In a nutshell, embedding flexibility into a data centre strategy is essential to ensuring the scalability and cost-effectiveness of the broader IT strategy.

Flexibility should be at the heart of every company's data centre strategy. In a world shaped by constantly evolving technologies and accelerating data consumption, those who are willing to adapt and keep pace with change are the most likely to see their strategies pay off.

Across the region, we can expect to see more and more businesses opting for greater flexibility by pivoting from on-premise to co-location and cloud-based IT hosting solutions. As cloud computing continues to gain prominence, hyperscale providers will be looking to aggressively expand to capture market share.

Given the growth in data centres, investors are increasingly looking to deploy their capital into this sector. The growing investor interest will lead to a very competitive environment for investment and options for enterprises looking for outsourced solutions. ■

Data Governance and the Board

By **PHILIP CHONG**, Partner, Risk Advisory, Deloitte



Data is growing in volume and importance across enterprises. The proper governance of data is an integral part of good corporate governance. This requires the frameworks and operating models to be on the board agenda.

Data is one of the most important assets of any enterprise, yet many organisations do not include the data perspective in their business planning and operations. As a result, data quality, usability, availability and integrity suffer. This can lead to mistrust, inefficiencies and heightened risks.

The proper care and handling of data by people as well as systems should be an important aspect of managing this important asset. With appropriate metrics, ownership and processes, data quality goals become part of everyday life and an integral part of operations.

Involving data stakeholders in data decisions empowers them with confidence in the data's integrity. This requires a thought-out approach to data governance.

Why organisations need data governance

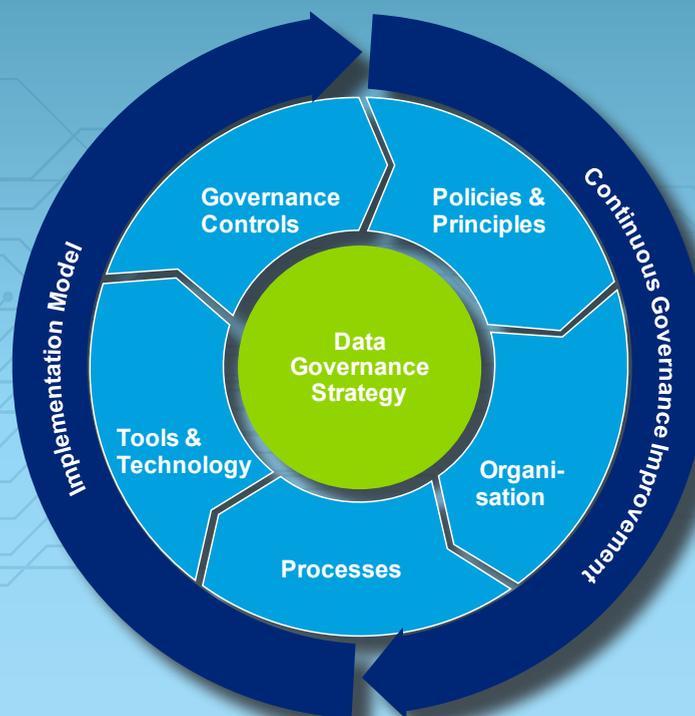
Data governance refers to the policies and processes by which an organisation manages the definition, use, quality, consistency, usability, security and availability of its data and information. It is about knowing the quality of data and that it is fit for use.

A data governance programme is about specifically managing data, based on meeting business requirements.

Data governance ensures the active involvement of data owners and users in the data management, quality and governance. This empowers data owners and users, assigning them accountability and ownership over the data they rely on.

Business decisions have to be supported by reliable data. The company's knowledge workers must have the data they need, when they need it.

Data Governance Framework



- **Policies & Principles** are guidelines and principles for enforcing data management standards and data governance processes.
- **Organisation** establishes roles and responsibilities, organisation structure and clear ownership for data management practice across different teams including decision-making bodies.
- **Processes** specifically outline how data is created, modified and maintained, enabling accurate data to be leveraged across the enterprise.
- **Tools & Technology** establish tools, data models, high-level architecture requirements, implementation options and roadmap to enable enforcement and adherence to recommended data management standards.
- **Governance Controls** identify the most important activities to be performed, measures progress towards achieving objectives and determines how well the governance and its processes are performing.
- **Implementation Model** includes implementation patterns, methods and engagement models.
- **Continuous Governance Improvement** establishes measures to review adherence to data management standards and processes, initiates improvement activities.

Source: Deloitte

Decision makers not only need to have the right information at the right time, but they need to have confidence in the accuracy and validity of that data for it to be effective.

Many organisations expend resources to migrate to new systems without considering the data requirements. The end result is that the data “mess”

of the old system is recreated in the new system which fails to deliver the promised advantages. Requirements for use and quality of the data need to be defined upfront, before implementation is considered.

Data deficiencies are risks to business stability, success and obligations.

For example, when organisations have teams that work in silos, duplicated information produces inconsistent and unreliable data that can make it difficult or impossible to deliver programmes. Working across the organisation to define common data requirements fosters common goals and enables efficient business development and service improvements.

Similarly, organisations must be equipped with policies and procedures. Staff training should be tracked, so that any data breach can be handled efficiently. Mishandling data can lead to embarrassing, costly and brand-damaging privacy, security and reporting breaches. Data users and owners that are involved in caring for data are better equipped to prevent costly breaches and to handle them if they do occur.

It is not enough to rely on a few key individuals and many “magic” spreadsheets. Having well documented data requirements, data definitions and data processes ensures that the organisation’s employees are working towards a common goal, and that information and knowledge are shared.

Enterprise risk is mitigated by being able to track, monitor, and consistently reproduce data performance.

Data governance framework

Data governance provides a structured and defined process that can be followed in a “business as usual” manner to involve the appropriate people in defining information requirements. Business needs drive data requirements and definitions, to influence information technology strategies and provide technical solutions, options and plans.

A data governance programme establishes information-centric processes across the enterprise and standardisation of shared concepts, such as consistent and sustainable

definition of business terms across systems and applications.

Employing a data governance framework and instilling diligence requires significant and sustained executive sponsorship, business collaboration and culture change management. In addition, several key processes around data issue management and monitoring need to exist to support the execution.

The right governance framework offers an end-to-end view of data governance. This framework forms the basis for better managing the entire data value chain across the organisation from quality, consistency, storage, usability and security perspective, (see box on “Data Governance Framework”).

Supporting the framework is an operating model that describes how data governance actually works. It includes an organisation structure, roles and responsibilities, interaction model, standards and processes (see box on “Data Governance Operating Model”).

The data governance operating model must have the power to mandate the Data Governance Office and all other data governance resources to perform the roles and responsibilities required to manage data as an enterprise resource and asset. All parties performing data governance or management activities must be accountable for the successful performance of their roles.

Role of the board

The board should clarify roles, accountabilities, and decision-making processes for management of data within the organisation, with focus on the following:

- Decision principles. Clear guidelines for decision-making roles, processes and behaviours, and a common language to facilitate cross-functional communication.

Data Governance Operating Model

1. Board and Senior Management.

- Ensure that data is managed as a corporate asset.
- Set data strategy in keeping with business strategy.
- Set the tone for the organisation.
- Allocate resources to support data governance efforts.

2. Data Governance Committees.

- Subject area owners with deep understanding of the data requirements to meet the business needs of their functional area.
- Collectively set priorities for data activities across the organisation.
- Design resources.
- Ratify policy.

3. Data Owners.

- Responsible for key data domains that define their success.
- Control over data definitions, data requirements, terms of use.
- Data quality requirements, accessibility, availability.

4. Data Stewards.

- Subject area experts with a deep understanding of functional area business needs and enterprise data requirements.
- Responsible to the data owners.
- Evaluate change requests, set data definitions and data requirements, monitor data quality, define data cleansing and data remediation.

5. Data Governance Office.

- Provides leadership and oversight for the data governance programme.
- Ensures appropriate execution and monitoring over the data governance programme.
- Maintains data governance documentation.

- Decision rights. Exact nature of each individual's role in decision processes that provide clarity, eliminate ambiguity and reduce cycle time.
- Management committees. Defined group of individuals who meet with a common mandate. Decision-making authority may not rest with the committees.
- Enablers. Organisational systems that propel or block effective decisions, such as processes, policy, systems and organisational structures.

The proper use of enterprise data is a concern for the board. In addition to the review and endorsement of the data governance framework and operating model, the board's agenda on organisation strategy needs to align with strategic, regulatory and privacy requirements for data.

Data that supports the enterprise reduces corporate risk and fosters growth. ■

Raising the Digital Competency of the Board

By ALVIN CHIANG and JYNN GOH



Globally, digital representation on boards has increased, with a growing number of directors appointed specifically for their technical skillsets and competencies. Expertise in technology and familiarisation with digital trends, however, should not be confined to just a few members of the board.



The bursting of the dot-com bubble in the late 1990s pushed the mandate of building of technology and digital competencies in boards to the back seat. However, with the embedding of the Internet of Things into our daily lives, and the advent of Industry 4.0, the tide is turning.

Recent years have seen a resurgence in technical director appointments on boards, as companies grapple with digital disruption brought about by new technology-enabled business models and changing consumer behaviours.

Companies today are, in one way or another, tech companies. Even traditional brick-and-mortar businesses are hard-pressed to adopt some form of digitisation in order to remain competitive. Best-in-class companies have both the board and management teams aligned towards the organisation's digital strategy.

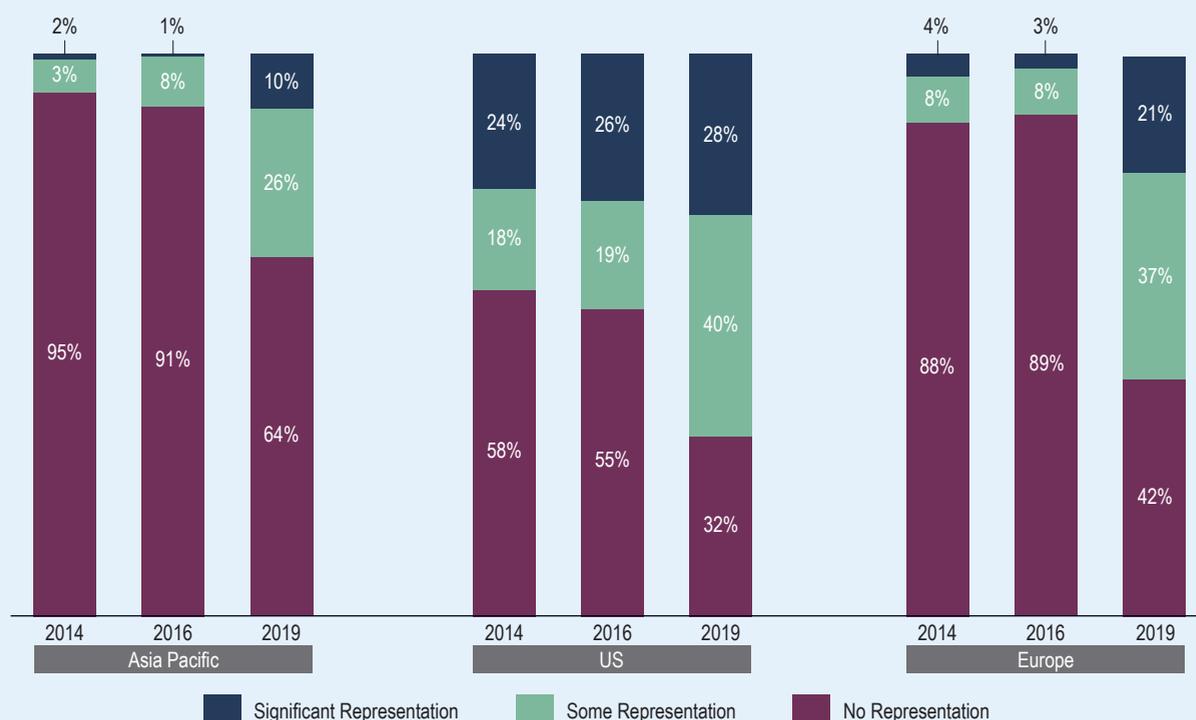
Research points to an increasing consensus that board leadership and engagement are absolutely essential in this respect: 53 per cent of respondents in Russell Reynolds Associates' *Digital Pulse Survey 2018* feel that the board is critical to the success of the organisation's digital initiatives, compared to 27 per cent in 2017.

Gearing up for the digital revolution

The good news is that we are seeing significant increases in digital representation on boards across all companies.

Analysis of the 300 largest publicly traded companies around the world based on the S&P Global 1200 shows that in Asia Pacific today, 26 per cent (8 per cent in 2016) of companies have a director with some form of tech background on their board, while another 10 per cent (1 per cent in 2016) have two or more such directors, (see box, "Digital Representation on Boards – Comparison Across Geographies").

Digital Representation on Boards – Comparison Across Geographies



Source: *Digital Pulse Survey 2018*, Russell Reynolds Associates.

It comes as no surprise that most Asia Pacific companies with digital representation on their boards are in the technology, financial services and industrial sectors (see box, “Digital Representation on Boards – Comparison Across Industries”). Companies like Tencent, SoftBank and TSMC are at the forefront with three tech directors each. That said, companies in the other more traditional sectors like manufacturing and retail are not sitting still, and have also started to incorporate more tech-savvy directors onto their boards.

Finding the right fit

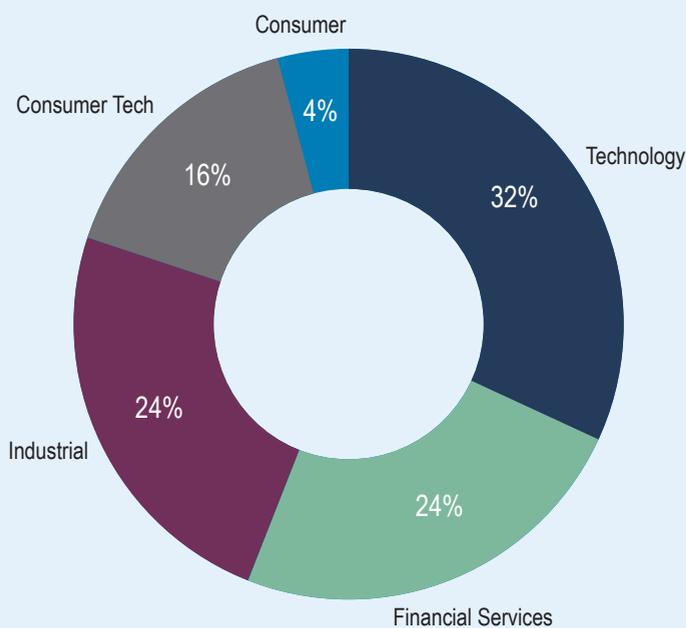
Broadly, tech directors tend to have executive experience in technology and in board work (see box, “Typical Profile of a Tech Director”). But exactly what kind of tech director a board will need will differ across organisations, depending upon the business of the company, the extent of its digital journey and its current board composition.

It is therefore important that boards have a holistic and honest review of the company to ensure compatibility. That said, there are five areas for a board to ponder over when seeking to add another member who can help guide tech transformation in the business (see box, “Five Areas to Consider Before Appointing the Next Tech Director”).

Companies may consider taking additional steps in the process of searching for directors to ensure that appropriate individuals are found. Psychometric assessments and evaluations may prove useful in determining the span of their competencies and personalities, while the team conducting the search ought to have adequate technical and board experience.

Introductory events for first-time board members allow potential and current board members to meet in a less informal environment.

Digital Representation on Boards – Comparison Across Industries



Source: Digital Pulse Survey 2018, Russell Reynolds Associates.

Typical Profile of a Tech Director

- Gender: 86% male, 14% female
- Age: 63.2 years old
- Number of current board appointments: 2.1
- Tenure as director: 5.2 years
- Management experience: 54.2% possess CEO experience, while the rest have general management experience. Those with CEO background have sat on 4.9 boards throughout their career compared to 1.9 for those without.
- Founded a business: 17.1%

Source: Digital Pulse Survey 2018, Russell Reynolds Associates.

Five Areas to Consider Before Appointing the Next Tech Director

1. What are the expectations of the board when it comes to tech expertise?

It is not the role of the board to execute transformation. Rather, it needs sufficient expertise and know-how such that it can provide oversight and advice, knowing when to rely on the experts, and to make sure the right questions are getting the right answers, especially from the business perspective. That means that tech directors must also be comfortable in contributing to a wide variety of strategic topics beyond technology.

It therefore comes as no surprise that many companies would favour a technology company chief executive officer (CEO), who knows both technology and business, over a deep subject matter expert, such as a chief technology officer (CTO) or chief information officer (CIO), when it comes to choosing new board members.

2. What are the specific areas which need strategic guidance and expertise?

Answering this question requires the board to understand where the company is in its technology journey and where it hopes to go.

Is the company in need of a sweeping overhaul of enterprise technology to become more efficient, or is it facing pressure to better engage with customers through digital tools – or both? Is it a traditional company – say, insurance or manufacturing – that is looking to jumpstart innovation efforts? Or a technology company looking to move into new verticals? Or is there a specific issue, like cyber security, e-commerce, or monetising digital services, that dominates all else?

The answers can often help a board choose between a technology expert and someone

who has overseen digital initiatives in another executive capacity.

3. Does the candidate have the right experience for what the company needs?

In the rush to infuse technology expertise into the board, some boards are willing to take nearly any executive from a company like Apple, Facebook or Google. However, it is important to look beneath the surface to ensure the candidate has the right experience and skills to contribute to board-level discussions on a range of topics.

Conversely, boards often overlook candidates who have exceptionally relevant experience in overseeing a transformation at a company in a more traditional industry, such as the insurance or automotive sectors. While people with this kind of experience may not look like a technology expert on the surface (for example, they may be the chief financial officers or heads of human resources rather than CIOs), their guidance on when and where to invest or pull back can be invaluable.

The key questions are: Has the candidate experienced multiple cycles of technology investments at another company that successfully shifted business models? Can he or she translate that experience into useful questions or guidelines for the board to ensure management is making the right bets?

4. Is the company (really) open to a new director profile?

The reality is that the board candidates with the deepest experience in digital business models tend to have less overall business experience than the average board member, and often come from organisations

with different cultures from those that are considering them as a board member.

Research shows that globally, the average director with technology experience is about four years younger than his or her traditional counterpart. In some cases, it can mean a distinct difference in seniority within directors' primary organisations, or journeys to their current roles.

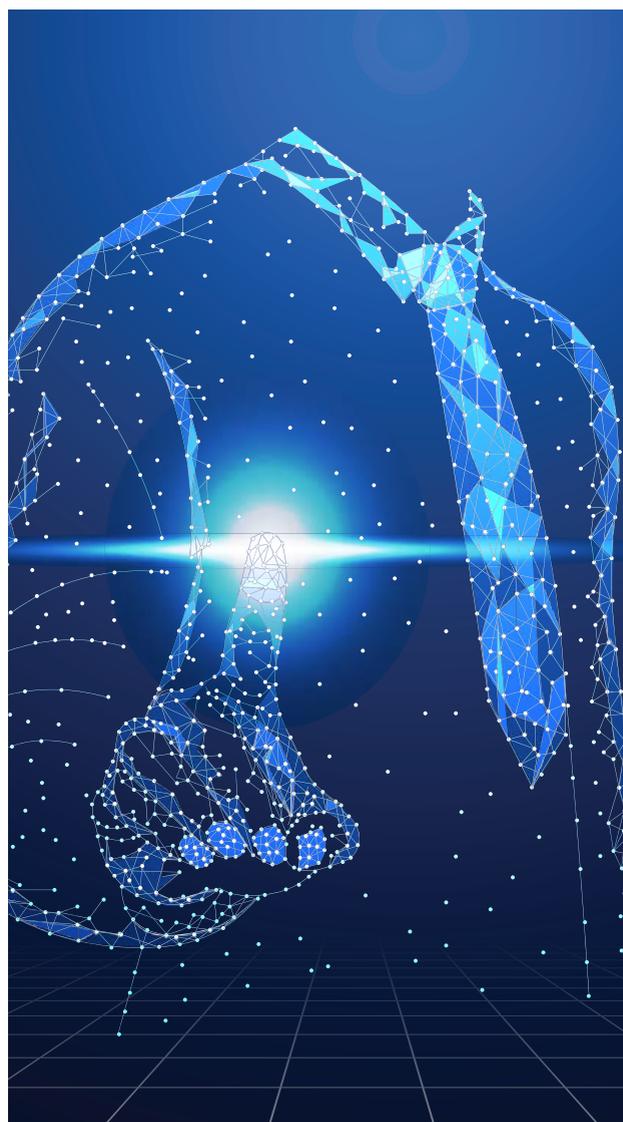
However, in Asia Pacific, there is no significant difference between the average age of all directors and tech directors in particular. This suggests that companies in the region prefer directors with more years of experience, yet this would likely come with trade-offs.

5. Is the candidate expected to be the main source of tech expertise on the board?

Appointing a director with tech expertise is generally just one part of a board's role in strengthening the company's technology strategy. That's in part because one person typically cannot cover every area of interest. It's also for liability reasons: Few directors want to feel they are dependent on the views of a single peer to make major decisions.

What is reasonable to expect from a director who is designated as a technology expert is that he or she will be an effective voice for change, particularly if that person is tasked with convincing a reticent CEO that big changes are necessary, or educating a less-savvy group of incumbent directors.

In such cases, subject-matter expertise needs to be balanced with a propensity to persuade and even disrupt; qualities that careful behavioural interviewing can unearth.



All hands on deck

All in all, the key is to look for directors who are fit-for-purpose, rather than expecting technical directors to be the be-all-and-end-all solution to technology transformation.

Successful strategic change is the mandate of the board working alongside the management team and stakeholders. To do so, it is crucial that boards have broader involvement to understand technology in the business of the company. ■

Alvin Chiang and Jynn Goh are Consultants at Russell Reynolds Associates.

The Evolving Role of the Board in Cyber Security

By **LEE SHIH YEN**, Senior Vice President, Ensign Labs, Ensign InfoSecurity

Cyber security management is an enterprise-wide issue that requires a shift in organisational culture, and the board must take a strategic role in its oversight.

Cyber security is fast becoming a vital conversation in the boardroom. With cyber criminality posing numerous challenges to businesses, it is not just an information technology issue. Cyber risk governance is a business mandate, requiring the full attention of directors.

But what are the areas that the board should probe into for good cyber governance?

1. Who's responsible for what?

Clearly defining cyber security responsibilities within the organisation is the board's top priority. Once these roles have been articulated, the board can set the organisation's attitude towards cyber risks, and hold the management accountable for the effectiveness of their cyber security programmes (see box, "Roles and Responsibilities").

2. What is the company's risk appetite?

Not all threats can be prevented. The board should take it upon itself to understand the organisation's tolerance to specific risks, and how they might impact business objectives – revenue, equity, productivity, brand reputation, among others.

Risk management discussions should identify all business assets, and categorise them based on their consequence severity levels. Critical business assets, which typically have high consequence severity, must always be prioritised. The general rule is that risks associated with critical assets should not be accepted.

3. What is the ROI of cyber security investments?

Cyber security spending may not always be a cost to the business. Each business is different. Based on the criticality of assets identified, the board must evaluate the financial, operational and legal costs of specific breaches. Once a proper risk assessment has been performed, the board must ask for a cost-benefit analysis to justify the appropriate allocation of funding and personnel to cyber security.

4. How are third-party vendors assessed for compliance?

One area that is often neglected is the supply chain. It can be a backdoor for threat actors to infiltrate the company's critical systems and steal information. To ensure security, the board must ask for their third-party vendors' proof of compliance to regulations and international standards, such as ISO27001 for information security management.

5. What crisis management activities does the company have?

Inculcating a security-first mindset is no easy task. But one key method is to constantly reinforce and practise it through attack simulations and table-top exercises. Everyone must be aware of what to do when a breach occurs. There's no time for second-guessing and hesitation. That means a response plan must be clearly defined, way beforehand.

6. How is the company as a whole adhering to compliance policies and processes?

With countries enacting policies and regulations

Roles and Responsibilities



CHIEF INFORMATION SECURITY OFFICER (CISO)

The CISO is responsible for the organisation's information and data security. This includes:

- Helping the board understand potential security issues that might occur from business decisions.
- Overseeing security policies, programmes and operations.
- Implementing security architecture that supports the organisation's business goals.



CHIEF RISK OFFICER (CRO)

The CRO is in charge of establishing the organisation's cyber security risk management programme. Some responsibilities include:

- Safeguarding critical financial and risk data.
- Assessing and ranking assets according to their risks.
- Ensuring the organisation is compliant with regulations.



CHIEF FINANCIAL OFFICER (CFO)

The CFO oversees the organisation's financial and accounting matters. Increasingly, this encompasses:

- Communicating to the board the return on investment (ROI) of cyber security spending.
- Determining how much cyber security insurance the organisation needs.
- Ensuring that the IT and security budgets are allocated to maximise impact on business priorities.
- Assessing the cost-benefit of cyber security investments.



CHIEF HUMAN RESOURCES OFFICER (CHRO)

People are the weakest link in cyber security. Hence, the CHRO plays a vital role in enforcing a cyber security culture within the organisation. This includes:

- Educating employees on cyber security's best practices.
- Ensuring that employees' and applicants' data are properly secured.
- Promoting cyber security awareness throughout the organisation.

that now impose legal implications when breaches occur, organisations are tasked to implement tighter policies and processes that ensure compliance and governance.

In Singapore, the two main laws that govern data protection are the Cybersecurity Act, and the Personal Data Protection Act. If the organisation sells products and services in the European Union (EU), as well as collects and handles personal data from EU residents, the General Data Protection Regulation should also be adhered to.

It is important for the board to understand how these laws affect the way their organisations handle data, making sure that adequate policies and processes are in place. The board should review if these laws are being followed, at least annually.

As complex as cyber security is, with the right governance, processes and protocols in place, organisations will be able to keep the "bad guys" at bay. But the board must also play its part by asking the management questions to provoke the right mindset, and build a sustainable and efficient cyber defence posture. ■

Data Protection – Taking the “It Will Happen” Approach



By LYN BOXALL

SID
SINGAPORE
INSTITUTE OF
DIRECTORS

**BOARDROOM
MATTERS**

Recent events have driven home the importance of data protection, especially of personal data. For example, in early 2018, it emerged that consulting firm Cambridge Analytica had misappropriated the personal data of millions of Facebook users without their consent. The information was then manipulated for political campaigning, with the intention to influence election outcomes.

This was a wake-up moment for the world.

“Data breach”, previously confined to accidental loss of personal data, suddenly raised the spectre of intentional fraud and exploitation on an unprecedented global scale.

Closer to home, in 2018, up to 1.5 million SingHealth patients’ records were stolen, including information on outpatient dispensed medicines records, in what was termed as Singapore’s most serious breach of personal data. Less than six months later, it was revealed that in a separate incident, the personal data of HIV-positive patients on the official medical registry had been compromised.

Penalties

The consequences of data loss may involve financial penalties.

Fines handed out by the Personal Data Protection Commission (PDPC) of Singapore are relatively

low. In the three years 2016 to 2018, the PDPC took enforcement action against 64 organisations and imposed fines totalling S\$339,000. In 2019, enforcement was scaled up, and 50 organisations were fined a combined total of S\$1.54 million.

The biggest fine the PDPC can dish out is S\$1 million – which it did to SingHealth and its provider, Integrated Health Information Systems, in 2019. Other jurisdictions are less forgiving. British Airways was ordered to pay an eye watering fine of £183 million (S\$320 million) in July 2019. It was the biggest penalty to be handed out under new rules provided by the European Union’s General Data Protection Regulation (GDPR).

The GDPR lists a set of principles relating to the processing of personal data and states that the controller (the organisation that determines the means and processing of personal data) “shall be responsible for, and be able to demonstrate compliance with, [those principles]”. The penalty for failing to do so is up to €20 million (S\$30 million) or four per cent of total worldwide annual turnover, whichever is the higher.

Accountability obligation

In July 2019, the PDPC published its Guide to Accountability under the Personal Data Protection Act, and announced that the “openness obligation” would be updated to the “accountability obligation”. Specifically,

accountability in relation to personal data protection is now defined as the undertaking and demonstration of responsibility for personal data in an organisation's possession or control.

An organisation demonstrates accountability by having developed and implemented a systematic framework for compliance with data protection laws within the organisation.

Such a framework includes compiling a personal data inventory for the organisation, mapping the flows of personal data within the organisation and to third parties, identifying the compliance risks in such flows and then devising written policies and standard operating procedures to manage those risks. Accountability is also demonstrated by records of staff being trained in them and by records of regular compliance audits.

In the past, the need for compliance with laws and regulations has been based on taking a passive, "checklist" approach. If nothing goes wrong, the checklist is obviously working; otherwise, the checklist needs to be tweaked.

Role of the board

Why should boards be concerned?

The cost is not just the fines, which may seem small (at this time), especially for large corporations, but the reputational and other damage, and the cost of clean-up, for instance.

The PDPC's Guide to Accountability states that: "A key step to ensuring a commitment to accountability is to embed personal data protection into corporate governance as the involvement of senior management is crucial."

As part of corporate governance, the role of the board is thus particularly relevant in personal data protection. The board must ensure that

management has the necessary budget and headcount resources and implements the processes necessary for the organisation to demonstrate its compliance with data protection law.

The board should lead accountable – responsible – organisations to embrace data protection as a core value that is embedded into corporate culture and processes.

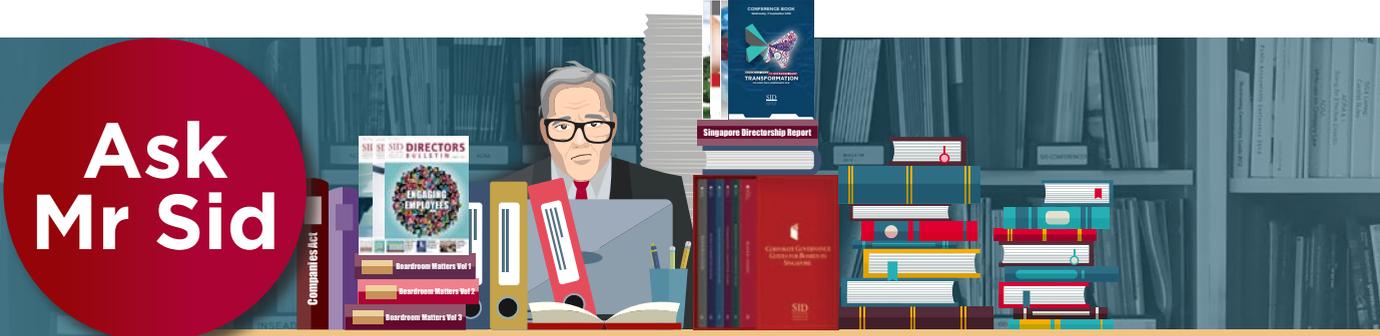
Shareholders expect the value of their investment in the company to be maintained. Fines in Singapore are not the real risk to shareholder value. Loss of reputation, brand damage and loss of customer trust are real pain points that can decimate shareholder value.

In addition, where there is a regulatory investigation, its costs are very real even where there is no regulatory penalty imposed. Senior staff are distracted from their business priorities that generate revenue and the costs of consultants to assist in the investigation can easily run into six figures.

Personal data protection is becoming a differentiator in an increasingly competitive market. Brand and reputation count. In this landscape, with a heightened sensitivity among customers about whether an organisation can be trusted to protect their personal data, customers can always take their business elsewhere if they suspect that the organisation does not treat their data with the respect and seriousness it deserves.

Boards which cling to the approach of "It won't happen to us", must wake up to the changing reality and business landscape. They should accept and prepare for the situation where "It will happen to us". ■

The writer is a former member of the Professional Development Committee of the Singapore Institute of Directors.



Ask Mr Sid

Dear Mr Sid

Re: Too Much Data About Data

It seems that all the talk these days is about data.

Sure, data is important. I get enough good, timely and adequate data to be able to make informed decisions in the boardroom. As a non-executive director, isn't that all that should matter to me?

For starters, the listed company of which I am a board member is in the hospitality industry. We own a chain of restaurants, and the main concern is to provide quality affordable fare. We may use data to keep track of our restaurants' sales performance, but we are not a technology firm.

So, I don't know why we have to get into the deep end about what kind of data the company has, and how it stores and processes them. We hire a bunch of technology specialists to deal with such matters.

Even so, we're overwhelmed by data issues. We keep hearing about the new data rules and regulations. And privacy concerns. And data breaches. And cyber security. I forgot

what PDPA stands for, but it hangs over us like a sword.

Virtually all of us directors really don't know our zettabytes from our troglodytes. We come from an age when data was what's in the phone book. It's just not practical or possible for the board to even try to keep up with the technology and laws around data.

Of course, we understand that our customer data has some value and needs to be protected, but the tech team take cares of it. They submit regular audit reports and seem to have it under control. We have not experienced any cyber attacks or hacking incidents. So, what's the big fuss about "Big Data"?

Mr Sid, is this something we need to worry about, any more than what we already do?

Yours sincerely

No-More-Data-Please



Dear No-More-Data-Please

While I understand the topic may fatigue you, data is a rapidly evolving area with grave impact on companies in so many ways.

There are, of course, different types of data. It could simply be the information you are provided with in the boardroom to help you and your fellow directors make decisions.

Today, however, data is defined more broadly. Often, it refers to computer data which is information that's captured, stored and processed electronically. It's the growth of such data that has led it to being called "Big Data".

Consider this:

- A zettabyte is a measure of storage capacity and is 1021 (1,000,000,000,000,000,000) bytes or 1 sextillion bytes. Imagine, if each gigabyte in a zettabyte were a brick, 258 Great Walls of China could be built.
- Data growth has been exponential. Experts estimate that the global datasphere, defined as the total data created, captured and replicated globally, reached 33 zettabytes in 2018, and will reach 175 zettabytes by 2025.
- A host of factors are causing this data growth: increasing internet and mobile usage, prevalence of Internet of Things, cloud computing backed by data centres,

and increase in virtual and augmented reality traffic. The imminent adoption of 5G cellular network technology will further drive such growth.

Sorry to provide you more data about data, but yes, the unabated growth of everything "data" in the digital economy is capturing attention. And for good reason: it creates boundless opportunities, but there are also significant challenges.

Opportunity

The value of data, as you have pointed out, is that it informs decision making.

The massive amounts of data now available means that the quality of decision making can be considerably enhanced, especially if the data is harnessed in ways not possible before.

What differentiates big data from the "regular data" you have been analysing to date are the tools used to collect, store and analyse the data in its increased volume and complexity. These tools include artificial intelligence (especially machine learning), data management, data mining, text mining, data analytics and Hadoop.

Even though you are not a technology company, you can avail yourself of such tools to collect and mine the considerable data

you have (and can have) about, say, your customers' spending patterns, and suppliers in your restaurant business.

In the past, sales forecasting was based primarily on metrics such as customer demographics, or past sales performances. With data analytics, you can better profile your customers and their tastes to inform your marketing campaigns, and configure your operations to suit and target different types of sales (takeaways vs catering vs premise sales, and food types).

You could also have a greater understanding of your suppliers' performances at a more granular level, which might lead to greater operational efficiency and cost savings on the part of many other businesses.

In other words, the possibilities for new uses of data are as manifold as the new recipes you can conjure up in your restaurants.

Challenges

The challenge of big data though, as you pointed out, is that there's too much of it. Hence the need for sophisticated tools to help sort through them. But data tools and storage are not cheap, and sorting through the complexities is not easy.

So, the first decision you need to make is what and how much of the data to capture and store before high quality research can begin. This is a matter on which the board should help set the direction.

A greater concern would be data security. Data breach and abuse are costly, not just in terms of the cost of fixing them and disruption to operations, but also in reputational damage.

And in today's world, cyber attacks are routine. You may think you have not been hacked, but the cyber security experts will tell you that your company has likely already been breached – you just don't know about it. IBM's research indicates that the average time between a breach and detection is over 200 days.

With privacy and confidentiality concerns, there are now legal requirements for the protection of personal data across the world. In Singapore, the primary legislation ensuring this is the PDPA (it stands for "Personal Data Protection Act"). But it's not the only legislation on data protection. The obligations of organisations for data protection are also set out in the Computer Misuse Act, Cybersecurity Act, Spam Control Act, Protection from Online Falsehoods and Manipulation Act and Banking Act, to name a few.

Role of the board

In the face of the prevalence of big data and its significant benefits and challenges to the organisation, it would be hard for you and the board to take a minimalist approach to data governance and use.

Data governance is the overarching strategy to ensure that the data the company has and uses is clean, accurate, usable and secure. This includes the proper management and ethical use of the data. And these are not just technical issues; they also impact and involve the business.

Yes, data governance and usage are jobs for management, but as the governing body of the company, the board has the duty to oversee it. Some questions you should be asking management are:

- Does the company have the skills and capabilities to deal with big data?
- Is the organisation complying with all the relevant laws, especially on data protection?
- How is the organisation managing security risks?
- What are the business opportunities afforded by big data, and how are these being progressed?
- What is the return on investment on big data?

To be effective in overseeing management, the board itself needs to understand big data, and set the tone for its protection and exploitation for business benefit.

Towards this end, the board should first upgrade directors' understanding and skills in technology and data. Some boards explicitly ensure that there are digital directors on the board, and form technology advisory panels.

The board should also look for opportunities to use big data in its decision making. You can, for example, use big-data visualisation technologies to make key governance decisions.

If it's any consolation, the data suggests that the majority of directors have yet to fully appreciate the importance of data governance and its link to good and effective corporate governance. You can be ahead of the curve if you choose to.

Yours sincerely



Mr Sid ■

Who is Mr Sid?



Mr Sid is a meek, mild-mannered geek who resides in the deep recesses of the reference archives of the Singapore Institute of Directors.

Burrowed among his favourite *Corporate Governance Guides for Boards in Singapore*, he relishes answering members' questions on corporate governance and directorship matters. But when the questions are too difficult, he transforms into Super SID, and flies out to his super network of boardroom *kakis* to find the answers.

Mr Sid's References (for this question)

Audit Committee Guide

Section 6.5: Data Analytics

Boardroom Matters

Vol 1, Chapter 13: "Board Alert for the Personal Data Protection Act" by Yeoh Oon Jin

Vol 1, Chapter 14: "Data Protection: Turning Compliance into Opportunity" by Lyn Boxall

Vol 2, Chapter 30: "Safeguarding Businesses from Digital Threats" by Yeoh Oon Jin

"Data Protecting – Taking the 'It Will Happen' Approach" by Lyn Boxall

SID Directors Bulletin

2016 Q3: "Digital Directors, Get on Board" by Audrey Tan

2016 Q4: "Seizing the Cyber Security Challenge with Data Stewardship" by Siobhan Gorman

SID Courses

Business Future Series 1: Disruptive Technologies for Directors

Business Future Series 2: Cyber Security for Directors

The AC Seminar 2020

Looking Beyond the Veneer of Numbers

With audit accountability in the spotlight, speakers and panellists at the sixth Audit Committee Seminar called for greater scrutiny of financial statements by ACs. A higher degree of oversight is needed to maintain the integrity of the financial reporting system, which plays a vital role in investor protection and, by extension, ensuring the proper functioning of the capital markets.

The annual seminar, jointly organised by ACRA, SGX and SID, was held at Parkroyal on Marina Bay, Singapore on 16 January 2020. More than 300 directors and professionals turned up for the event. The theme this year was “Looking beyond the Veneer of Numbers”.

In his opening address, Mr Ong Khiaw Hong, CE, ACRA, underscored the increasing criticality of good corporate governance to the capital

market and the importance of upholding integrity of financial statements against the backdrop of geo-political, economic and social uncertainty. He outlined steps taken by ACRA to strengthen audit reporting, and emphasised the need for all stakeholders to work together.

Ms Bong Yap Kim, Divisional Director of Financial Reporting Division, ACRA, shared the findings from ACRA’s Financial Reporting Surveillance Programme. She highlighted what



ACs should look out for during their review of financial statements.

Ms Ng Meow Ling, Chief Inspector, Practice Monitoring Department, ACRA, outlined how ACs could leverage on the Audit Quality Indicators disclosure framework to make better-informed decisions in their evaluation of auditors and facilitate meaningful conversations between ACs and their auditors.

Ms June Sim, Head of Listing Compliance, SGX RegCo, updated on the proposed disclosure guidelines to be incorporated into the Listing Rules to enhance the reporting standards and disclosure for valuations. Through case studies, she pointed out areas that ACs and boards should pay attention to, including the nine-year threshold for directors, quarterly reporting and announcement matters.

Mr Ng Siew Quan, Partner, Corporate Governance Leader, PwC Singapore, explored the challenges facing ACs, including changing accounting standards, evolving regulatory and legal environment, increasingly complex transactions, and evolving business models that

present new risks. He described situations that warrant the attention of ACs and what they could do in such situations.

A panel discussion on “What the Numbers Aren’t Telling You” ensued, moderated by Mr Soh Gim Teik, Chairman of the AC Chapter, SID. The four panellists were: Mr Patrick Ang, Managing Partner, Rajah & Tann Singapore LLP; Ms Veronica Eng, Independent Director, Keppel Corporation; Mr Kelvin Tan, Independent Director and AC Chairman, UnUsUaL Ltd, and Mr Ng Siew Quan. They shared insights into how ACs could make sense of the increasingly complex data and obtain additional insights through alternative means, before taking questions from the floor.

In his closing address, Mr Tan Boon Gin, CEO, SGX RegCo, addressed the issue of “trust deficit” and outlined how proposed measures by SGX RegCo are aimed at enhancing oversight of the quality of work of auditors and property valuers in respect with their dealings with listed companies.

The key takeaways from the seminar are summarised in the following pages.



ACRA Regulatory Updates

Findings from Financial Reporting Surveillance Programme

- A consistently high proportion (9%) of financial statements had modified audit opinions in FY 2017 and FY 2018.
 - ACs to resolve issues upfront and work towards receiving clean audit opinion so that investors can have reliable financial information.
- From cases reviewed, the key root causes of non-compliance were:
 - (a) The lack of knowledge or expertise.
 - ACs to engage professional valuer for the valuation of complex instruments and conduct impairment tests.
 - ACs to use ISCA's guidance on real estate valuation to facilitate compliance with the financial reporting standards and reduce differences in practices.
 - (b) Some cases suggest intention to achieve a desired outcome.
 - ACs to consider management intention when reviewing accounting treatment.

Harnessing the benefits of Audit Quality Indicators (AQIs)

- Feedback from audit firms:
 - Need for mindset change – some ACs were more interested in audit fees.

- Need for qualitative analysis of AQIs to minimise misinterpretation.
- Preference for Project Management Indicators that are useful for recurring audits.
- Need for fit-for-purpose model, e.g. different operating environments and business models of firms; scale and complexity of financial reports that may lead ACs to form wrong conclusions when targets are not met.
- Changes to AQI Disclosure Framework:
 - AQI targets: replaced with industry data (range and average).
 - AQI on Audit hours: time spent by senior audit team members enhanced with time spent by each member according to grade and during various audit phases.
 - AQI on quality control (QC): absolute headcount in QC functions enhanced with relative headcount, i.e. QC headcount per 100 audit headcount.
 - AQI on Independence: removed.
- How ACs should interpret AQI information:
 - Understand facts of information and context in which AQIs are presented.
 - Evaluate AQIs as a whole, incorporating historical trends and comparisons across firms.
 - Ask pertinent questions and set expectations for audit.

“ ACRA and MAS have set up a joint forum, to coordinate efforts to better monitor and review accounting and disclosure lapses. This will enable both agencies to take errant companies to task more promptly.

Strengthening enforcement capabilities is essential to motivate stakeholders to act in the public interest and comply with the law. It provides the necessary deterrence against non-compliance, so that those who comply on their own do so in the knowledge that the system is fair to all. This sets the ground for regulators like ACRA to forge strong partnerships with stakeholders, to engender the right behaviours amongst stakeholders in the eco-system.”

Ong Khiaw Hong
CE, ACRA



“ We have no issue with short-cuts but they must lead to outcome that comply with the accounting standards.”

“As some accounting issues can be complex and judgemental, I cannot emphasise enough the importance of having members with deep accounting knowledge in the audit committees.”

Bong Yap Kim
Divisional Director, Financial Reporting Division, ACRA



“ Audit committees play a crucial dual oversight role. They not only ensure effective oversight over financial reporting by management; they also enhance interaction and oversight over external auditors to ensure high quality and reliable financial reports for the investors to enable the latter to make better informed decisions. High audit quality requires collective effort from all stakeholders.”

Ng Meow Ling
Chief Inspector, Practice Monitoring Department, ACRA



SGX RegCo Regulatory Updates

Nine-year Threshold for Independent Directors (IDs)

- If a person has been a director for an aggregate period of more than nine years as of 1 January 2022, he will not be deemed independent (and a new ID must be recruited within three months), unless his continued appointment as an ID has been sought and approved in separate resolutions, by way of a two-tier vote, prior to 1 January 2022 [LR 210(5)(d)].
- As of 1 January 2022, IDs must comprise at least one-third of the issuer's board, failing which vacancy must be filled within two and not exceeding three months.

Disclosure-based Regime

- Quarterly Reporting (QR):
 - As of 7 February 2020, Rule 705(2) states that only companies in the following situations will be subject to QR:
 - It has received a disclaimer of opinion, adverse opinion or qualified opinion from its auditors on its latest financial statements (FS).
 - Its auditors have expressed a material uncertainty relating to going concern on its latest FS.
 - SGX RegCo has regulatory concerns with the issuer.
 - Companies receiving modified opinions to provide the following in each of their QRs:
 - Updates on efforts to resolve each audit issue.
 - Board confirmation that each audit issue is adequately resolved.
 - Rest of companies are subject to financial reporting semi-annually.
- Announcement matters:
 - Rule 703(1) on disclosure of price-sensitive information does not apply when:

- A reasonable person would not expect disclosure of such information.
- The information is confidential.
- To disclose companies' near-term earnings prospect when there are:
 - Changes in prospects statements.
 - Changes in public information.
 - Material changes in business information.
- To disclose material transaction when:
 - Issuer is committed to the transaction.
 - Further negotiation on the transaction are pending.
 - Transaction is subject to precedent conditions that have yet to occur.
- To disclose letter of demand when:
 - Amount or action in letter poses a material impact.
 - Negotiations pending outcome of lawsuit are ongoing.
- Disclosure of trade secrets:
 - Trade secrets include intellectual property, specific processes or system.
 - Eroding companies' competitiveness is an invalid reason for non-disclosure.
- General pointers for announcement matters:
 - Provide adequate information to enable investors to make informed decisions.
 - Refrain from boilerplate statements.
 - Be open to questions during briefings or interviews.
 - Provide balanced and fair view in promotional materials, with only facts and no jargon.

Valuation Matters

- For real properties in Singapore: Property valuation reports to comply with standards set by Singapore Institute of Surveyors and Valuers.
- For real properties beyond Singapore: Property valuation reports to comply with International Valuation Standards.

“We note that 41 per cent of listed issuers have directors with over nine years of service on their boards. For boards of small sizes which have IDs with tenures of more than nine years as of 1 January 2022, I would advise them to go for re-election during the 2020 AGM. Even though the IDs would only be subject to the two-tier shareholders’ vote during the 2021 AGM, they run the risk of not being re-elected – which means the board would have to find a new ID within three months.”

June Sim

Head of Listing Compliance, Singapore Exchange Regulation



“Today, we launched our public consultations on a series of proposals aimed at enhancing our oversight of the quality of work of auditors and property valuers in respect of their dealings with listed companies.

These proposals are to deal with the trust deficit, which exists not just within the Singapore context, but also globally, particularly in respect of audits.”

“[In certain circumstances], The loss of confidence may be so overwhelming that the market refuses to accept the findings of the special auditor as being conclusive. At this point, everyone is in a difficult position. The statutory auditors may not want to resign.

The shareholders may not want to replace the auditors. The power to change the statutory auditors ultimately resides with the shareholders and not the regulators. But if nothing is done to resolve the impasse, the company may well succumb to a self-fulfilling prophecy.

In such a case, it may be necessary for us to direct a second audit which is akin to a re-audit. This additional auditor will review the overall financials of the company and provide a second audit opinion.”

“Some say, ‘It takes a village’. I say, ‘It takes a community’, and I look forward to working closely with even more of you to achieve our shared purpose and common goal, which is preserving the integrity of the market.”

Tan Boon Gin

CEO, Singapore Exchange Regulation



Piercing the Veil through Professional Scepticism

Challenges facing Audit Committees (ACs) today

- Changing accounting standards.
- Evolving regulatory and legal environment.
- Increasingly complex transactions.
- Evolving business models with attendant new risks.

Situations that call for greater scrutiny

- Diversification into new businesses:
 - Generating profits from the selected business model.
 - Additional expenses relating to new business operations.
 - Accounting treatment for new technology.
 - Different regulatory environment pertaining to international businesses.
- Business expansion and entry into new markets:
 - Mergers and acquisitions.
 - Legal and financial due diligence.
 - Valuation.
 - Realisation of value from post-merger integration.

- Market dynamics in new territories that may affect business operations.
- Write offs and Impairments:
 - Scrutinise company's approach towards impairment testing upon sensing a risk that assets may be materially impaired.

What ACs should look out for

- Monitor evolving standards and understand the implications.
- Evaluate the assumptions and judgement taken by management in pushing through deals.
- Focus on the caveats given by service providers for valuations.
- Ensure that audit plans are updated along with evolving business models.
- Ensure sufficient checks and balances over the CEO and senior management.

Summary

- Have a good understanding of the business, including the underlying details, and macro environment.
- Always verify and clarify when in doubt.

“On the present challenge of evolving regulatory and legal environment, you will note that the standards remain largely unchanged over the years. As to complex transactions, I pose the question to all companies: ‘Which deserving company out there does not have any complex business transactions?’ And regarding evolving business models, I presume it is the ambition of every company to have the intention to expand their businesses that may entail changing their business models. So, these so-called present challenges, strictly speaking, are not new. It may be merely that the arm of the law has become a little longer to clamp down on errant business practices.”

Ng Siew Quan

Partner, Corporate Governance Leader, PwC



Panel Discussion



L-R: Soh Gim Teik (Council Member, SID), Patrick Ang (Managing Partner, Rajah & Tan Singapore LLP), Ng Siew Quan (Partner, Corporate Governance Leader, PwC Singapore), Veronica Eng (Independent Director, Keppel Corporation), Kelvin Tan (Independent Director and Chairman Audit Committee, UnUsUaL Limited).

How to make sense of the numbers?

Soh Gim Teik, SID Council Member, Panel Moderator

“Audit committees really need to spend some time and get down to looking at the nitty gritty, and delve deeper into the basics. They need to understand the business model so that they are in a stronger position to question and/or challenge the management, should the need arise, and ensure they are doing the right thing.”

Mr Kelvin Tan

“From an investor’s perspective, four key material statements should be focused on: P&L (profit and loss), statement on cash flows, balance sheet and statement of comprehensive income. There should not be concentration on just one statement.”

“There is no one-size-fits-all formula. It depends on the company, the business model and the environment. Numbers are historical and need to be looked at in light of what is happening in the industry and the market. Single numbers don’t tell the whole story. We need to look at the totality of the situation.”

Ms Veronica Eng

“Cash is fact. Profit is opinion.”

Mr Ng Siew Quan

“The management perspective is very different from the board view, the latter which can be based purely on numbers. It is imperative for ACs to look beyond the numbers and have a solid understanding of the business.”

“Take China Aviation Oil for instance, it is a strong company in the business of bringing jet fuel into China. Trouble started brewing for them when they decided to go into a side business for which there was no proper structure. This was compounded by the fact that their board was inexperienced in that area. This led to the management taking short-cuts. None of these risks were reflected in the numbers whatsoever. Nonetheless, the report revealed business failure at every level.”

Mr Patrick Ang

Panel Discussion

What precautions can management take?

Mr Bernard Yeo, Independent Director, Sin Heng Heavy Machinery Limited



“To me, the most important quality is management integrity. Management’s relationship with the board is also key. At the same time, enforcement in the area of white-collar crime needs to be tightened.”

“Singapore may have made good progress on the corporate governance front but enforcement in the area of white-collar offences is weak and often has no teeth. It is high time we beef up in this aspect. While integrity is important, it is not a given and the arm of the law must be long enough to catch offenders of weak integrity.”

Mr Kelvin Tan

“Management is not a man for all seasons. Uncharted territory needs different skillsets and talent.”

“In circumstances where a company needs to change its strategy in order to survive, the board must assess whether the incumbent management team has the right mindset and the breadth of skillsets to take the company forward, within the timeframe required. Boards need to assess management on a regular basis. It does not necessarily mean removing the incumbent but could include actions to supplement/complement existing bench strengths with people of different capabilities or experience.”

Ms Veronica Eng

“In my course of work, I’ve observed that distressed clients often reach out for help at a very late stage, where there is a risk of the issues becoming intractable. A stigma exists in Asia against declaring trouble, and there is an instinct to conceal problems. It is a fear of being called out. Perhaps that is why most problems are often kept within a closely-knit group in management. But one must bear in mind that the sin of omission is akin to the sin of commission.”

“Boards need to ask themselves if they are asking the right questions, and acting fast enough, to address potential problems, before it’s too late. We need to be more proactive and prevent the situation from getting out of hand.”

Mr Patrick Ang

“Focus on the CEO and his management team. Strive to understand them. Ask yourself if you can trust them. If not, is it because the management is incompetent or dishonest?”

Mr Ng Siew Quan

Are we in a *déjà vu* moment, with the global financial crisis at our doorstep?

Mr Kyle Lee, Non-Executive Director, Great Eastern Holdings Limited



“One positive outcome is the “present truce” in the China-US trade friction. However, global debt and prices are on the high side. Low interest rates cover a lot of sins. Markets would do well to remember the lessons of over-exuberance and hubris, given that history often repeats itself.”

Ms Veronica Eng ■



Global Director Survey



Global Director Survey Reveals Big Data Concerns

Global research taking the pulse of board directors around the world shows directors are concerned about technological disruption, with Big Data as the top disruptor.



The findings from the inaugural *Global Director Survey 2018* by the Global Network of Director Institutes (GNDI), representing 130,000 directors, were released in September 2018.

A majority – 63 per cent – of directors around the world regard Big Data as the top technological disruption to their organisations. “Big Data” describes any voluminous amount of data that has the potential to be mined for information, including structured data (e.g. spreadsheets and databases) and unstructured data (e.g. social media posts, audio, video, emails, PDFs, digital images and GPS data).

While on their radar, however, many boards are not taking advantage of big data to improve organisational effectiveness, create value and make better decisions. Only 44 per cent of the respondents agreed that they used big data for decision making, while 28 per cent of directors surveyed do not use big data in their governance decision making.

Worryingly, only 53 per cent of boards say their boards understood about cyber security and the cyber risks of their organisation. While 61 per cent felt they have good or excellent understanding of their organisation’s data privacy practices, 37 per cent felt they had limited or no understanding.

Cautious optimism

The *Global Director Survey 2018* also took a snapshot of directors’ business confidence. The survey found 45 per cent of directors were “mostly confident” or “very confident” about prospects for growth over the coming year. Another 36 per cent were “moderately confident”. Private and listed companies were more confident than not-for-profit and government organisations.

Poverty and income inequality were among the major concerns of directors worldwide as the most pressing social and economic issues. In the Asia-Pacific region, housing and infrastructure were of particular relevance to directors, according to the survey results.

The survey

The *Global Director Survey* ran from May to June 2018. It was conducted on behalf of the GNDI by the Institute of Directors of New Zealand with the support of 16 other national director institutes including SID.

A total of 2,159 directors from 17 countries participated. More than half (53 per cent) sat on three to four boards which means they have a wide experience and broad insights. Of directors who responded, 36 per cent were on boards of private companies, 23 per cent were on boards of listed companies, and 22 per cent were directors of not-for-profit organisations.

Spotlight on the Corporate Governance of Data

The inaugural *Global Director Survey 2018* found that Big Data is considered by board directors all over the world to be the biggest disruptor. In conjunction with the report on the survey findings, the Global Network of Director Institutes (GNDI) issued its guidelines on the Corporate Governance of Data in November 2018.



The paper aims to provide high-level guidance to boards of directors on balancing legal and ethical considerations regarding data compliance and the need to maintain competitive advantage. It highlights core principles in providing strategic direction, oversight and the promotion of a data governance culture.

The guidelines are developed in consultation with its member institutes including SID. They cover

all data-related strategic commercial and operational activities of the company. An extract of the paper is presented on this and the next page.

The full version of the *GNDI Guidelines on the Corporate Governance of Data* and the *Global Director Survey Report* can be found at www.gndi.org.

GNDI Guidelines on the Corporate Governance of Data

Core Principles

Part I: Providing Strategic Direction for Data Governance

1. **Data strategy:** In line with the roles and responsibilities defined, the Board of Directors leads and supports the management in developing a comprehensive:
- Data business strategy.
 - Data resilience strategy (incl. compliance, risk and crisis approach).

That defines the company's approach to:

- Data asset management (incl. valuation and intellectual property approach).
- Data technology management.
- Data partnership management.

Based on the following data principles:

- Data safety and security.
- Data value and veracity.
- Data usability and compatibility.
- Data integrity and sustainability.

2. **Data strategy integration:** The Board of Directors ensures that relevant data considerations are fully integrated into other strategies, in particular into the:

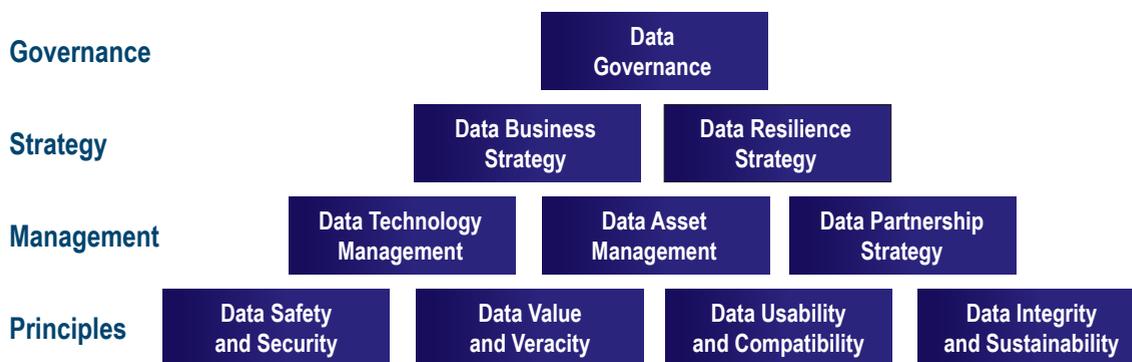
- Market-oriented strategies (e.g. marketing and sales, research and development).
- Operations-oriented strategies (e.g. manufacturing, procurement, logistics).
- Resource-oriented strategies (e.g. finance, human resources, technology / information technology, legal).
- Ecosystem-oriented strategies (e.g. partnerships, alliances, mergers and acquisitions).

Part II: Providing Oversight of Data Governance

3. **Data strategy execution:** The Board of Directors ensures that the data strategy is developed and implemented by the senior management as per plan and target by monitoring its implementation progress and measuring its impact, including benchmarking performance with that of comparable organisations.

4. **Legal data compliance:** The Board of Directors ensures that the company is fully compliant with all data regulations applicable wherever the company operates and data is stored (e.g. in

GNDI Data Governance Framework



cloud computing) and has the respective corporate policies and corresponding training programmes in place, in particular related to relevant:

- Data protection laws, industry standards and recommendations.
- Privacy laws, industry standards and recommendations.
- Cyber security laws, industry standards and recommendations.
- Intellectual property laws, industry standards and recommendations.

5. Ethical data compliance: The Board of Directors ensures ethical compliance and understanding of the social implications of its data-related business practices, in particular related to:

- Data-driven technologies (e.g. artificial intelligence).
- Data handling (e.g. data storage, leakage, veracity or sharing).
- Data use (e.g. research, sales and marketing and human resource management).

6. Data reporting: The Board of Directors understands the value of intangible data assets, as well as possible risks and liabilities from the use of data and ensures meaningful reporting in line with respective accounting rules and reporting standards.

Part III: Promoting the Culture for Data Governance

7. Data-driven governance: The Board of Directors promotes the concept of data-driven governance by utilising data technologies to improve transparency, effectiveness and efficiency of board decisions in a responsible manner.

8. Data awareness, mindset and capability building:

The Board of Directors ensures that the organisation develops awareness for data-related matters, a mindset for data-driven decision making and data handling capabilities across all levels of the organisation by ensuring adequate representation of experts in the relevant bodies, incorporation of data-related capabilities in competence framework and provision of training and development programmes, in particular in:

- Data methodologies.
- Data technologies.
- Data resilience management (incl. compliance and risk management).
- Data ethics.

Part IV: Adapting Data Governance to the Context

9. Contextual adaptation: The Board of Directors ensures that corporate data governance policies are adapted to local requirements and sectoral contexts (if the company operates in multiple markets and industries).

10. Regular updates: The Board of Directors ensures that data governance policies are regularly reviewed and adapted to take into account the latest technological, competitive and regulatory developments. ■

Cutting Through the Complexity of Risk Management

SID and KPMG conducted a session for over 60 participants on risk management practices and disclosures, at Capital Tower seminar rooms on 3 February 2020. The seminar was jointly presented by Mr Adrian Chan, Vice-Chairman of SID and Mr Irving Low, Partner and Head of Advisory at KPMG Singapore.

At the 2019 Singapore Corporate Awards, SID with the support of KPMG, launched the Best Risk Management Awards to recognise companies that have demonstrated adequate and effective risk management practices and established an adequate and effective risk management framework.

A panel, drawn from the representatives of the winners of last year's awards, included Mr Chan Kok Seong, Chief Risk Officer, United Overseas Bank, and Mr Leong Kok Ho, Chief Financial Officer, Tuan Sing Holding. They were joined



by Ms Poh Mui Hoon, SID Council Member, and Mr Yap Chee Keong, Independent Director, Olam International.

Mr Low acted as moderator for a wide-ranging discussion by panel members and participants, on the importance of identifying risk (especially downside risk), and having people and processes in place. Embedding a corporate culture that regards risk management as a core strategy, in light of changes to the business landscape, arising from technology, innovation and disruption, is critical. ■

AC Pit-Stop

Managing Risk in a Digital World

SID, in collaboration with The Institute of Internal Auditors, conducted a two-hour session for audit and board risk committee members, on "Managing Risk in a Digital World". Mr James Fong, Regional Business Director, RSA Archer, delivered the presentation to 30 participants at the seminar rooms of Capital Tower on 5 March 2020.

With a risky start to the decade, Mr Fong highlighted how digital transformation of businesses increases risk. In a *Fortune 500 2019 CEO Survey*, respondents ranked cyber security, technological change and increased regulation as the greatest challenges facing their business. Digital risk is defined as unwanted and often unexpected outcomes that stem from digital transformation, digital business processes and the adoption of related technologies.



Mr Fong explained how integrated risk management supports digital risk maturity in four key areas: cyber incident risk management, third-party governance, data privacy risk and digital business resiliency.

Everyone in the organisation has to own the risk. Engagement and accountability lead to improved collaboration, while data analytics and visibility support automated processes for greater efficiency. ■

SGOOD Advanced

Developing a Digital Mindset

SID kickstarted 2020 with its first SGOOD (Governance for Outstanding Organisation Directors) Advanced module: “Digitalisation and Innovation for NonProfit Organisations”. The session on 8 January 2020 was facilitated by Dr Francis Goh, CEO and Founder of Hehsed Consulting, and attended by around 20 board members of nonprofits. The venue was the National Volunteer & Philanthropy Centre.

Dr Goh explained how the everchanging and volatile business landscape has led to a new era, the Industrial Revolution 4.0, where digital dexterity is now the most sought-after business quality. Digitalisation and innovation thrive in organisations which embed a forward-thinking mindset and attitude into the organisational culture.

The participants discussed the “Five Thinking Processes”: conceptual, critical, strategic, system



and design. These thought processes can help nurture digital innovation and equip leaders with the ability to adopt and adapt a digital mindset for decision making.

The session concluded with a panel discussion where panelists Dr Kelvin Phua, CEO of SATA CommHealth and Mr Choo Jin Kiat, Executive Director of O’Joy Care Services recounted their personal innovation journeys and shared how they constantly try to empower and encourage their employees to adopt innovative thinking. ■

Branding for NPOs

SID presented its second SGOOD Advanced module: “Branding for NonProfit Organisations” on 18 February 2020. The session was facilitated by Mr Jorg Dietzel, CEO of Jorg Dietzel Brand Consultants Pte Ltd, and attended by 25 board members of nonprofits. The venue was the National Volunteer & Philanthropy Centre.

Mr Dietzel explained what drives consumers today and how brands can connect and communicate with consumers in the new “experience economy”. Participants learnt how not-for-profit brands can fit into the new environment of social experiences and apply digital outreach strategies to find new volunteers and donors.



The session concluded with a panel discussion where panellists Ms Beatrice Chen, Chairperson, Community Partnership Committee of AWWA, and Ms Georgette Tan, President of United Women Singapore, recounted their organisations’ branding journeys and shared the importance of building brand purpose and keeping the brand aligned to their mission. ■

Director Appointments

SID members appointed as directors of listed companies during the period 1 December 2019 to 29 February 2020

COMPANY	PERSON	DESIGNATION
Advancer Global Limited	Loy Soo Chew (Li Shizhou)	Independent Director
Asiatic Group (Holdings) Limited	James Yip Mun Foong	Independent Director
Bumitama Agri Ltd	George Lee Lap Wah	Independent Director
Chemical Industries (Far East) Ltd	Lim Yew Nghee	Non-Executive Director
DLF Holdings Limited	Foo Kia Juah	Independent Director
DLF Holdings Limited	Kok Cheang-Hung	Independent Director
Dyna-Mac Holdings Ltd	Lim Ah Cheng	Executive Director
Far East Orchard Limited	Alan Tang Yew Kuen	Executive Director
Figtree Holdings Limited	Francis Lee Fook Wah	Non-Executive Director
GS Holdings Limited	Zhang Rongxuan	Non-Executive Chairman
GSH Corporation Limited	Wendell Wong Hin Pkin	Independent Director
International Cement Group Ltd	Francis Wong Loke Tan	Independent Director
Jumbo Group Limited	Rachel Sim Yu Juan	Non-Executive Director
Keppel Corporation Limited	Penny Goh @ Lee Yoke Sim	Independent Director
Kitchen Culture Holdings Ltd	Alex Chua Siong Kiat	Independent Director
Kitchen Culture Holdings Ltd	Lau Kay Heng	Independent Director
LCT Holdings Limited	Mark Leong Kei Wei	Independent Director
Marco Polo Marine Ltd	Micheal Tan Hai Peng	Non-Executive Chairman
Metech International Limited	Chng Hee Kok	Independent Director
MS Holdings Limited	Kho Kewee	Independent Director
Nam Lee Pressed Metal Industries Limited	Yeo Siew Eng	Independent Director
Natural Cool Holdings Limited	Benjamin Choy Bing Choong	Executive Director
NauticAWT Limited	Aphichat Sramoon	Independent Director
NauticAWT Limited	Chirasak Chiyachantana	Non-Executive Chairman
NauticAWT Limited	Kunchit Singsowan	Independent Director
NauticAWT Limited	Lim Yeow Hua @ Lim You Qin	Independent Director
OEL (Holdings) Limited	Jeffrey Hing Yih Peir	Non-Executive Director
OEL (Holdings) Limited	Alice Zhao Xin	Executive Director
OEL (Holdings) Limited	Yap Koon Loong	Independent Director
Oversea-Chinese Banking Corporation Limited	Tan Yen Yen	Independent Director
Pine Capital Group Limited	Lee Sin Ann	Executive Director
Rich Capital Holdings Limited	Sovann Giang	Non-Executive Chairman
TEE International Limited	Alex Siow Yuen Khong	Independent Director
Thai Beverage Public Company Limited	Timothy Chia Chee Ming	Independent Director
USP Group Limited	Kelvin Tan Wee Peng	Independent Director
Zhongmin Baihui Retail Group Ltd	Benjamin Choy Bing Choong	Independent Director

INSEAD Closing Dinner • 12 December 2019



SID-SMU Directorship Programme Modules 1 & 2 • 7-9 January & 19-21 February 2020



Fundraising Tips & Best Practices • 14 January 2020



SID Lo Hei Lunch • 3 February 2020



Board and Director Fundamentals • 18 February 2020



Director Financial Reporting Fundamentals • 25 February 2020



SID's Q1 Events (Jan–Mar 2020)

DATE	TYPE	EVENT DETAILS
7-9 Jan 2020	PD	SDP1: The Role of Directors
8 Jan 2020	PD	SGA2: Digitalisation and Innovation for NPOs
14 Jan 2020	PD	MFG3: Fundraising Tips and Best Practices
16 Jan 2020	Event	ACRA-SGX-SID Audit Committee Seminar
3 Feb 2020	Event	Best Risk Management Award Seminar
3 Feb 2020	Event	SID Lohei Lunch
18 Feb 2020	PD	BDF: Board and Director Fundamentals
18 Feb 2020	PD	SGA3: Branding for NPOs
19-21 Feb 2020	PD	SDP2: Assessing Strategic Performance
25 Feb 2020	PD	DFE: Director Financial Reporting Fundamentals
4 Mar 2020	PD	LED1: Listed Entity Director Essentials
5 Mar 2020	PD	ACP: Managing Risk in a Digital World
11 Mar 2020	PD	LED2: Board Dynamics
17 Mar 2020	PD	LED3: Board Performance
19 Mar 2020	PD	LED4: Stakeholder Engagement
24 Mar 2020	PD	SGD1: Essentials of NonProfit Board Leadership
25 Mar 2020	PD	LED5: Audit Committee Essentials
25-27 Mar 2020	PD	SDP3: Finance for Directors
27 Mar 2020	PD	LED6: Board Risk Committee Essentials
27 Mar 2020	PD	LED7: Nominating Committee Essentials
31 Mar 2020	PD	LED8: Remuneration Committee Essentials

Upcoming Events

Core Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
NBF: NonProfit Board and Director Fundamentals	3 Apr 2020	0900 to 1700	Clarke Quay Central
SDP1: The Role of Directors	7-9 Apr 2020	0900 to 1730	SMU Campus
BFS1: Disruptive Technologies for Directors	15 Apr 2020	0900 to 1300	Raffles City Tower
SGD2: Board Dynamics	17 Apr 2020	0900 to 1300	Clarke Quay Central
QLED: Qualified Listed Entity Director Assessment	21 Apr 2020	1000 to 1200	Capital Tower
EGP: Enterprise Governance Programme	21 Apr 2020	0900 to 1300	Capital Tower
BFS3: Artificial Intelligence and Ethics for Directors	22 Apr 2020	0900 to 1300	M Hotel
MCD3: The Board in Strategy Formulation	28 Apr 2020	0900 to 1730	M Hotel
CTP2: Building Business in the Digital Era	29 Apr 2020	0900 to 1100	Capital Tower
QLED: Qualified Listed Entity Director Assessment	29 Apr 2020	1000 to 1200	Capital Tower
QLED: Qualified Listed Entity Director Assessment	6 May 2020	1000 to 1200	Capital Tower
LED1: Listed Entity Director Essentials	13 May 2020	0900 to 1700	M Hotel
SDP2: Assessing Strategic Performance	13-15 May 2020	0900 to 1730	SMU Campus
SGA5: Fundraising	15 May 2020	0900 to 1300	Clarke Quay Central
LED2: Board Dynamics	15 May 2020	0900 to 1300	M Hotel
LED3: Board Performance	19 May 2020	0900 to 1300	M Hotel
SYD: So, You Want to be a Director	20 May 2020	1030 to 1300	Capital Tower
LED4: Stakeholder Engagement	21 May 2020	0900 to 1300	M Hotel
SGD3: Board and Management Dynamics	28 May 2020	0900 to 1300	Clarke Quay Central
CTP3: Business Thinking for Sustainability	28 May 2020	0900 to 1100	Capital Tower
SGA4: Cyber Security and Data Privacy for NPOs	10 Jun 2020	0900 to 1300	Clarke Quay Central
IDP1: Board Fundamentals – Responsibility, Effectiveness, Decision Making and Strategy	14-17 Jun 2020	0900 to 1730	INSEAD Campus
QLED: Qualified Listed Entity Director Assessment	17 Jun 2020	1000 to 1200	Capital Tower
IDP1: Board Fundamentals – Responsibility, Effectiveness, Decision Making and Strategy	17-20 Jun 2020	0900 to 1730	INSEAD Campus
QLED: Qualified Listed Entity Director Assessment	19 Jun 2020	1000 to 1200	Capital Tower
QLED: Qualified Listed Entity Director Assessment	23 Jun 2020	1000 to 1200	Capital Tower
CTP4: Emerging Risk of Weaponised Digital Disinformation	24 Jun 2020	0900 to 1100	Capital Tower
MCD1: Boards and Political Networks	25 Jun 2020	0900 to 1300	M Hotel
SGD4: Talent and Volunteer Management	26 Jun 2020	0900 to 1300	Clarke Quay Central
BDF: Board and Director Fundamentals	30 Jun 2020	0900 to 1730	M Hotel
DFF: Director Financial Reporting Fundamentals	1 Jul 2020	0900 to 1700	Capital Tower
SDP3: Finance for Directors	1-3 Jul 2020	0900 to 1730	SMU Campus
SYN: So, You Want to be a NonProfit Director	7 Jul 2020	1700 to 2100	Clarke Quay Central
SYD: So, You Want to be a Director	8 Jul 2020	1030 to 1300	Capital Tower
LED1: Listed Entity Director Essentials	16 Jul 2020	0900 to 1700	M Hotel
SGA6: 5 Things a NonProfit Director Must Know	16 Jul 2020	0900 to 1300	Clarke Quay Central
LED2: Board Dynamics	17 Jul 2020	0900 to 1300	M Hotel
LED3: Board Performance	17 Jul 2020	1330 to 1730	M Hotel
LED4: Stakeholder Engagement	20 Jul 2020	0900 to 1300	M Hotel
LED5: Audit Committee Essentials	20 Jul 2020	1330 to 1730	M Hotel
LED6: Board Risk Committee Essentials	21 Jul 2020	0900 to 1300	M Hotel
LED7: Nominating Committee Essentials	21 Jul 2020	1330 to 1730	M Hotel
LED8: Remuneration Committee Essentials	22 Jul 2020	0900 to 1300	M Hotel
CTP5: Executive and Director Remuneration	23 Jul 2020	0900 to 1100	Capital Tower
SGD5: Strategy and Board Performance	28 Jul 2020	0900 to 1300	Clarke Quay Central
MCD4: Enterprise and Strategic Risk Management	13 Aug 2020	0900 to 1300	M Hotel
SDF: Startup Director Fundamentals	20 Aug 2020	0900 to 1200	Capital Tower
SGD6: Financial Management and Accountability	25 Aug 2020	0900 to 1300	Clarke Quay Central
QLED: Qualified Listed Entity Director Assessment	26 Aug 2020	1000 to 1200	Capital Tower
CTP1: Sustainability Deciphered for Business	27 Aug 2020	0900 to 1100	Capital Tower
SDP4: Risk and Crisis Management	27-28 Aug 2020	0900 to 1730	SMU Campus
QLED: Qualified Listed Entity Director Assessment	3 Sep 2020	1000 to 1200	Capital Tower
QLED: Qualified Listed Entity Director Assessment	11 Sep 2020	1000 to 1200	Capital Tower
SGD7: Fundraising, Outreach and Advocacy	22 Sep 2020	0900 to 1300	Clarke Quay Central
IDP2: Board Dynamics, Efficiency and the Role of Committees	22-24 Sep 2020	0900 to 1730	INSEAD Campus
BFS2: Cyber Security for Directors	24 Sep 2020	0900 to 1300	Kallang Place
SDP5: Strategic CSR and Business Valuation	24-25 Sep 2020	0900 to 1730	SMU Campus

Core Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
BDF: Board and Director Fundamentals	29 Sep 2020	0900 to 1730	M Hotel
IDP2: Board Dynamics, Efficiency and the Role of Committees	30 Sep-2 Oct 2020	0900 to 1730	INSEAD Campus
MCD2: Cross-Cultural Leadership and Competence	2 Oct 2020	0900 to 1300	M Hotel
LED1: Listed Entity Director Essentials	6 Oct 2020	0900 to 1700	Parkroyal Collection Marina Bay
LED2: Board Dynamics	8 Oct 2020	0900 to 1300	Parkroyal Collection Marina Bay
LED3: Board Performance	8 Oct 2020	1330 to 1730	Parkroyal Collection Marina Bay
LED4: Stakeholder Engagement	13 Oct 2020	0900 to 1300	Parkroyal Collection Marina Bay
LED5: Audit Committee Essentials	15 Oct 2020	0900 to 1300	Parkroyal Collection Marina Bay
LED6: Board Risk Committee Essentials	15 Oct 2020	1330 to 1730	Parkroyal Collection Marina Bay
LED7: Nominating Committee Essentials	1 Oct 2020	0900 to 1300	Parkroyal Collection Marina Bay
LED8: Remuneration Committee Essentials	21 Oct 2020	1330 to 1730	Parkroyal Collection Marina Bay
SGD8: Social Trends	27 Oct 2020	0900 to 1300	Clarke Quay Central
DF: Director Financial Reporting Fundamentals	4 Nov 2020	0900 to 1700	Capital Tower
SDP6: Effective Succession Planning and Compensation Decisions	12-13 Nov 2020	0900 to 1730	SMU Campus
QLED: Qualified Listed Entity Director Assessment	18 Nov 2020	1000 to 1200	Capital Tower
QLED: Qualified Listed Entity Director Assessment	24 Nov 2020	1000 to 1200	Capital Tower
QLED: Qualified Listed Entity Director Assessment	27 Nov 2020	1000 to 1200	Capital Tower
IDP3: Developing Directors and Their Boards	14-16 Dec 2020	0900 to 1730	INSEAD Campus
IDP3: Developing Directors and Their Boards	15-17 Dec 2020	0900 to 1730	INSEAD Campus

Other Professional Development Programmes

PROGRAMME	DATE	TIME	VENUE
BDC4: Nominating Committee Chairman's Conversation	7 Apr 2020	1200 to 1400	Shangri-La Hotel
ACP: Intangible Assets in a Tangible World	16 Apr 2020	0900 to 1100	Hong Leong Building
BDC3: Board Risk Committee Chairman's Conversation	27 Apr 2020	1200 to 1400	St Regis Hotel
ACP: Reviewing Financial Statements and Selecting Auditors	26 May 2020	1000 to 1200	SGX Auditorium
BDC1: Board Chairman's Conversation	3 Jun 2020	1200 to 1400	Shangri-La Hotel
BDC2: Audit Committee Chairman's Conversation	11 Jun 2020	1200 to 1400	The Fullerton Hotel
ACP: Leveraging Analytics and Technology for Internal Control and Fraud Prevention	9 Jul 2020	0900 to 1100	Wilkie Edge
BDC5: Remuneration Committee Chairman's Conversation	24 Aug 2020	1200 to 1400	TBC
ACP: Impact of International Tax Rule Changes	17 Sep 2020	0900 to 1100	Marina One
BDC6: CEO Conversation	29 Oct 2020	1200 to 1400	TBC

Major Events

EVENT	DATE	TIME	VENUE
SID Annual Golf Tournament	12 Jun 2020	0930 to 2100	Sentosa Golf Club
Singapore Corporate Awards	23 Jul 2020	1700 to 2200	Resort World Sentosa
Singapore Governance and Transparency Index Launch	4 Aug 2020	0900 to 1100	1 Raffles Place
SID Directors Conference 2020	9 Sep 2020	0900 to 1600	Suntec City Convention and Exhibition Centre
Annual Corporate Governance Roundup	17 Nov 2020	1000 to 1200	Orchard Rendezvous Hotel

NOTICE

In view of the evolving 2019-novel Coronavirus (Covid-19) situation, SID is taking precautions to reduce the risk of community spread. We will be implementing extra measures, including temperature taking and requests for travel declaration and personal details for contact tracing.

We apologise for any inconvenience, if some courses are fully subscribed or postponed. All other SID courses and events will proceed as usual, unless otherwise advised.

We will continue to monitor the situation and update members accordingly. Registrants who have signed up for any affected courses will be notified by email on the status of their registration.

Do look out for our updated course schedule on our website and our email updates.

For enquiries, please contact us at 6422 1188 or email us at events@sid.org.sg.

Course dates and venues are subject to change. Please refer to www.sid.org.sg for the latest updates.

Welcome to the Family

December 2019

Murray Dangar Bell
Barun Boudh
Annabelle Cai Xinyu
Steven Alan Carroll
Dylan Jude Castagne
Derrick Chan
Chan Shiok Faun
Chang See Hiang
Francis Chong Wai Siak
Benjamin Choy Bing Choong
Lucas Aditya Djunaedy
Guan Yeow Kwang
Han Lu
Michael Henry
Vilen Kachalov
Koh Choon Fah
David Christopher Kuo
Lincoln Kwok Chung Chieh
Francis Lee Yaw Loong
Amy Lin Xiaoming
Eugene Liu Hern Choon
Ritesh Maheshwari
Manoj Nathani
Ng Kheng Choo
Phi Van Nguyen
John Nielsen
Ong Kar Ching
Lawrence Pek Eng Leong
Kiran Raj
Wallis Ranatunga
Andrew Seit
Cedric Stadelmann
Tan Bee Bee
Paul Tang Wei-Min
David Peter Walker

Edmond Wong
Ken Wong
Floyd Patric Wood
Yeo Hock Chye
Zhang Rong Xuan

January 2020

Benjamin Abbott
Shawn Ang Hoe Hui
Chan Wai Man
Eric Chan Ying Kuen
Adeline Chang Pei Li
Chen Guang
Tushar P Doshi
Fang Zhixiang
Fu WenXing
Roger Goh Hock Hin
Adeline Hoe
Koh Poh Soon
Valerie Kok
Wayne Koo Kim Heng
Gio Lee Foo Han
Lee Sze Yeng
Kenneth Lim Kee Eng
Lucas Ignatius Loh Jen Yuh
Michael Mark Mah Kai Leong
Vijay Kumar Maheswari
Maszenan Bin Abdul Majid
Sueanne Darlee Mocktar
Ng Beng Tiong
Gunananthan Nithyanantham
Ong Su Faye
Ferhad Patel
Gordon Perchthold
Terence Quek
Gaurav Sanan

Gurbinder Singh
Jeremy Tan
Kenny Tan Chuan Huat
Tan Lye Huat
Adrian Tan Theng Wai
Alan Tang Yew Kuen
Jackie Thia
Edgar Masa Tindoy
Passorn Tumrongsiskul
Victoria Wu Ying Ying
Gordon Yeo
Yeong Wai Cheong
Lena Yong Oi Ling

February 2020

Pravi Bansal
Martin Brown
Chan Su Yee
Alan Cheah
Chia Beng Kwan
Chandrima Das
Yves De Laet
Jonathan Eu Zai Jie
Penny Fang Chen Chun
Han Chung Heng
Sandra Interdonato
Gurcharan Singh Kadan
Sunil Kumar Karapanahalli Ranganatha
Adeline Kee
Koh Jin Kiat
Gerard Lai
Clara Lee
Lee Sin Ann
Lim Ah Cheng
Joni Lim Rui Ping

Lim Yew Nghee
Jeffrey Loh
Munib Madni
Sarang Mahajan
Haider Manasawala
Gayathri Peria
Jaya Moorthi Pillai
David Robinson
Eric Saux
Andrew Benjamin Seck
Si Wei Wei
Juhi Singh
Benjamin Smith
Siti Suriah Taib
Georgette Tan
Tan Wei Tze
Michael Tang
Tay Yew Thiam
Teh Leong Kok
Iris Teo
Amitabh Thard
Babu Paul Thekkumkudiyil
Frederic Thieltgen
Rajesh Tibrewal
Fabio Tiviti
Timothy Toh
Wendell Wong
Richard Yap Beng Tat
Yap Koon Loong
Andrew Yeo
Ben Yeoh
Yong Joon Fai
Zhao Xin

SID Governing Council 2020

CHAIRMAN

Tham Sai Choy

SECOND VICE-CHAIRMAN

Adrian Chan

COUNCIL MEMBERS

Wilson Chew

Ferdinand de Bakker

Junie Foo

Philip Forrest

Pauline Goh

Theresa Goh

Derek Lau

Howie Lau

Lee Suan Hiang

Max Loh

Ng Wai King

Neil Parekh

Poh Mui Hoon

Jaspal Singh

Soh Gim Teik

Tan Boon Gin

FIRST VICE-CHAIRMAN

Wong Su-Yen

TREASURER

Ramlee Buang



CORPORATE GOVERNANCE

International Directors Programme



INSEAD is one of the world's leading and largest graduate business schools with campuses in France, Singapore and Abu Dhabi. With 165 renowned faculty members from 41 countries, INSEAD brings a global perspective and cultural diversity in all aspects of its research and teaching and to become "The Business School for the World." Every year, more than 11,000 corporate leaders and executives participate in INSEAD's various educational offerings. The INSEAD Corporate Governance Centre harnesses INSEAD's expertise in multiple disciplines for a comprehensive and sustainable response to the challenges facing directors today.



The Singapore Institute of Directors (SID) is the national association of company directors. It works closely with regulators and other stakeholders of the corporate ecosystem to uphold and enhance the highest standards of corporate governance and ethical conduct. SID supports the professional development of all directors (private, listed, international and nonprofit) in their directorship journeys (aspiring and new directors to board chairmen). SID also provides thought leadership on corporate governance and directorship issues through research, publications, and the Singapore Corporate Awards.

EXCELLENCE IN BOARD PRACTICES

The Singapore Institute of Directors has partnered with leading business school INSEAD and the INSEAD Corporate Governance Centre (ICGC) to bring the acclaimed International Directors Programme to Asia.

The International Directors Programme seeks to develop more effective directors for the increasingly-complex governance challenges presented by dynamic global markets.

The programme consists of three modules of three days each. The International Directors Programme is designed to take directors to the next level by going beyond compliance and focusing on excellence in board practice. Upon completion of the programme, participants may apply for the INSEAD Certificate in Corporate Governance, the first truly international qualification for board members from an academic institution.

NEXT SESSIONS

June 2020 (1)

- Module 1: 14–17 June 2020 in Singapore
- Module 2: 22–24 September 2020 in Fontainebleau
- Module 3: 14–16 December 2020 in Singapore

June 2020 (2)

- Module 1: 17–20 June 2020 in Singapore
- Module 2: 30 September–2 October 2020 in Singapore
- Module 3: 15–17 December 2020 in Singapore

More sessions available in Fontainebleau, France.

Please visit www.insead.edu for further details.

IN ASSOCIATION WITH:



Institut Luxembourgeois des Administrateurs

Founding partners: PWC, Institut Luxembourgeois des Administrateurs, Russell Reynolds, Singapore Institute of Directors

Go beyond compliance and achieve excellence in board membership:

www.insead.edu/international-directors-programme

Tel: +33 (0)1 60 72 41 27

Modern Governance

Turn governance into a
competitive advantage

The practice of empowering leaders
with the technology, insights, and
processes required to fuel good governance.

diligent.com



Diligent

a **MODERN
GOVERNANCE**
company