Board discussions
What NEDs have been debating

September 2018

pwc

Contents

Introduction

PwC's programme for Non-Executive Directors includes a series of briefings, workshops and other events to help address the need to keep up to date with Board level issues. This document summarises the discussions arising from our events over the past six months.

The season began with briefings on **The workforce of the future,** exploring how technology is changing the way we work at a rate faster than ever before and looking at what this might mean for future worlds of work. In keeping with this technology theme, an early evening event in April focused on **Eight essential emerging technologies,** those technologies deemed to have the most impact on business when viewed in terms of relevance, global reach, technical viability, market size and the pace of public and private investment.

Another early evening panel discussion in April looked at **Delivering total deal value**. M&A can be one of the most effective ways of building value for an organisation but often does not deliver the full potential and the session reflected on how this could be improved.

Another strategic topic was the subject of our May briefings on **China's Belt and Road Initiative.** This is a vast, interconnected infrastructure and related ecosystem project, notable not just for its scale but also for its timeframe. It provides opportunities for businesses to partner with the Chinese on different projects in a variety of ways and could spark a 21st Century expansion of global economic growth, technology exchange and, inevitably, Chinese influence.

Risk remains a constant feature of the Board agenda and we continue to focus on different aspects of this topic. A recent early evening event saw Anthony Fitzsimmons, Chairman of Reputability LLP, exploring **Rethinking reputational risk.** The discussion looked at how reputations which take time to build can be destroyed in an instant and why seemingly well-respected organisations unexpectedly fail.

Our summer workshop season continued to include sessions on **Cyber security** as this remains firmly on Board agendas. The first workshop covered a broad landscape of cyber security basics – setting context, explaining why this is a Board issue and providing a framework to help NEDs think about the key areas. The second explored seven principles for cyber security governance as well as a deeper dive into four key areas – developing a business perspective, assessing current state, improvement recipes and handling incidents and crises.

Still in the realm of technology, a new workshop explored **Blockchain and cryptocurrencies – applications and risks.** This considered some of the business applications of blockchain, the rise of cryptocurrencies, the regulatory environment and expected future developments.

A further workshop looked at **Social media, digital tools and online hygiene for NEDs** from an individual perspective to help NEDs determine what type of online profile they might wish to have, since there is no avoiding developing a digital footprint in today's world. At the same time, the issue of 'online hygiene' to reduce exposure to breaches was explored, given that NEDs frequently sit on multiple Boards and sometimes work remotely using their own technology.

For those NEDs with a charity in their portfolio, a workshop addressed **Charities – how to adapt and thrive in the current climate.** This was an opportunity to discuss some of the key considerations for charities including impact, reputation management, effective use of resources, collaboration and making difficult decisions.

Developments for **Audit Committees** – which continue to have a full agenda – were not overlooked. A series of update workshops provided a technical accounting update and a review of developments in corporate governance and reporting, as well as sessions exploring upcoming climate-related financial disclosures and the future of audit.

For those on **Remuneration Committees** there were workshops looking at the continuing focus on executive pay by the Government, the media and the public at large. Trends and an update from the recent AGM season were discussed, in addition to a consideration of the new UK Corporate Governance Code recommendations relating to executive pay.

In all of the workshops and briefings, there was considerable debate, with sharing of ideas on the topics and discussion around the roles NEDs can play in their Boardrooms. The combination of expert knowledge with the sharing of experiences with peers adds real value to these sessions, and I would like to thank all those NEDs who participated in our various events. We will continue to focus on matters featuring on Board agendas and look forward to further insightful discussions over the next six months of the programme.

Andy Kemp
Chair, Non-Executive Director programme
andy.kemp@pwc.com
September 2018

The workforce of the future

Technology is changing the way we work at a rate faster than ever before. Automation and artificial intelligence are replacing human tasks and jobs, as well as changing the skills that organisations are looking for in their people.

PwC's recent 'Workforce of the future' report draws on research begun in 2007 and a specially commissioned survey of 10,000 people in China, India, Germany, the UK and the US. It develops 'four worlds of work' for 2030 to prompt thinking about different possible scenarios that could develop and therefore how best to prepare for the future.

Presenter:

Carol Stubbings

PwC partner

carol.a.stubbings@pwc.com

Need to know

- The pace of change due to technological developments is unprecedented in what is now a truly global world.
- Future different worlds of work and the '100 year life' mean that current systems and infrastructure around the workforce will not be fit for purpose going forward.
- Automation and artificial intelligence are likely to replace 30% of tasks freeing up capacity for other opportunities.
- Different skills, such as leadership and emotional intelligence, will be more highly valued going forward.
- The need to attract and retain talent will be critical.
- Companies and their Boards need to be taking action now to consider what this means for their organisations going forward.

Context

The session began with some context-setting around the pace of change due to technological developments. Undoubtedly, the world is changing at a rate faster than ever before. At the beginning of the century, Ray Kurzweil, futurist and chief engineer at Google, predicted that 20,000 years of progress would be crammed into the next 100.

Global megatrends and uncertainty

It is the collision of the five global megatrends:

- technological breakthroughs
- demographic shifts
- shifts in global economic power
- rapid urbanisation
- resource scarcity and climate change

and the impact that humans have, that makes things interesting and challenging. Technology of itself is neither good nor bad but the way people use it can be critical.

There is existing tension between individualism, where 'me first' rules, and collectivism where fairness and equality prevail. At the same time, there is tension between corporate integration with big businesses dominating and business fragmentation where the traditional barriers to entry have been removed allowing new players to quickly establish themselves.

In this uncertain environment:

- 56% of people think governments should take 'any action needed to protect jobs from automation'
- 37% are worried about automation putting jobs at risk.

Four worlds of work

In 2007, PwC had begun research looking at how the world was changing to come up with a framework and vision for the workforce in 2020. In 2017, it was realised that much of what had been predicted to happen by 2020 had already occured so the research was updated with a survey of 10,000 people in China, India, Germany, the UK and the US.

This led to the outlining of four possible worlds of work, which will not necessarily operate in isolation, by 2030. It is clearly impossible to know how the future will unfold but doing nothing, given the pace of change, is no longer an option and the four worlds prompt thought around planning for the future

The four worlds are:

The blue world – Corporate is king

- Big company capitalism rules as organisations continue to grow bigger and individual preferences trump beliefs about social responsibility.
- There is sustained performance with highly talented individuals and automation driving profitability.

The green world – Companies care

- Social responsibility and trust dominate the corporate agenda with concerns about demographic change, the climate and sustainability becoming key drivers of business.
- The green world focuses more on purpose and societal impact. Some 'blue' companies are already aspiring to this.

The red world – Innovation rules

- Organisations and individuals race to give consumers what they want. Innovation outpaces regulation.
- Digital platforms give outsized reach and influence to those with a winning idea.
- Specialists and niche profit-makers flourish. These organisations are fastest to market, with innovation key. They solve a problem and then move on.

The yellow world – Humans come first

- Social-first and community businesses prosper.
- Crowdfunded capital flows towards ethical and blameless brands.
- There is a search for meaning and relevance with a social heart.
- Artisans, makers and 'new Worker Guilds' thrive and 'humanness' is highly valued.

In the recent survey, many respondents were attracted to the green and red worlds, whilst most people wanted to live in a yellow world. If bright individuals start opting out of the corporate world, where will organisations get their talent?

The changing workforce

Whichever of these worlds, or combinations thereof, prevail workforces and their aspirations are undoubtedly changing. This is particularly true with the overlay of the 100 year life where people expect to be working longer and have 8/9 jobs over their lifetime. Millennials and subsequent generations now have different aspirations.

In previous decades, the following was the typical set-up for a couple:

1960s – career + homemaker

1980s – career + job

Today – dual career

However, many things that are currently provided to the workforce as a result of these previously existing models are becoming outdated. The shape of the workforce needs reconfiguring and organisations will need to think about how to engage with older workers and how to attract younger workers.

Impact of artificial intelligence (AI)

Although each of the four worlds is different, through each runs the thread of automation and the implications of robotics and AI. CEOs agree that this is likely to require:

- a new balance – with automation of tasks
- adaptability – people need to be agile and willing to change
- pivotal talent – the ultimate prize.

There is a great deal of fear and uncertainty around automation and AI among workforces and companies need to be communicating better about this. The key is to stop thinking in terms of jobs as a whole and to think instead about individual tasks where the following questions are asked:

- can we automate
- can we augment
- can we offshore
- is a person needed?

It may be that 30% of tasks (rather than jobs) can be automated and this frees up some of the individual's time for other, more creative, activities.

There are also different levels of AI:

- assisted intelligence is here today and is automating repetitive, standardised or time-consuming tasks and providing assisted intelligence
- augmented intelligence is rapidly emerging with humans and machines collaborating to add value
- autonomous intelligence in the future will permit adaptive continuous intelligent systems to take over decision making with the future of humans at work in doubt.

However, AI cannot operate in isolation and collaboration, plus jobs that we may not yet be able to envisage, will be created to replace the tasks that are automated. Historical skill sets may not be what is needed going forward and leadership and emotional intelligence will be highly valued.

It is worth noting that a number of high profile organisations now require their people to work in their offices, rather than from home, as they recognise the power of human collaboration. They have built campuses like small cities to be able to meet all of their employees' needs on site.

Another organisation has appointed a 'director in charge of resources' as opposed to the traditional HRD, since resources are now likely to encompass the gig economy, off-shoring, robots, etc., as well as the human workforce.

Purpose will become increasingly important to help with retention of a more contingent workforce and organisations will need to live and breathe their values.

Implications for Boards

The future is here today but many businesses have a short-term focus. Organisations need to take action now with an understanding of the disruption that is out there. Six key messages for leaders of companies are:

- **Act now** – change is already happening and accelerating
- **No regrets and bets** – plan for a dynamic future with multiple and evolving scenarios and make 'no regrets' moves that work with most scenarios plus some big 'bets'
- **Own the automation debate** – automation and AI will affect all levels of the organisation and cannot be left to IT/HR
- **People not jobs** – whilst organisations cannot protect jobs which are automated, they have a responsibility to their people in terms of nurturing agility and retraining
- **Build a clear narrative** – anxiety destroys confidence and the willingness to innovate so there should be a clear and open debate around the topic.

Specific questions NEDs should consider in their Boards are:

- Has the Board identified alternative future scenarios?
- Has the organisation identified how automation and workforce decisions deliver or undermine their purpose, societal trust, customer experience and organisational culture?
- Does the Board understand how automation will impact the volume, types and value of jobs?

Open forum Q&A

The open forum Q&A was wide-ranging and covered the following areas:

Question	*Answer*
What will the effect be on pay/wages? Do the models generate enough wealth for what society will need?	There will definitely be an impact and different types of skills, e.g. creativity, may be worth more going forward. Governments and society will need to determine whose responsibility it is to retrain those whose jobs are automated. In a red or yellow world, people will earn what they can, whilst in blue or green, there could be more gig workers and movement from one to another. Blockchain could be used to record all skills and experience making individuals more portable with 'highest bidder' type auctions. An individual still needs purpose and meaning so a universal basic income may not be the answer.
With the shifts in global economic power, will Chinese/Indian multinational companies have the same approach to values?	Many Chinese nationals are going back to China from western universities and there is a need for more global curiosity. Developing countries are no longer copying the West but also creating and innovating.
Many of the digital superpowers have come out of the US or China and Europe has not yet produced a contender – why?	There may be a lack of purposeful innovation in Europe, possibly because there are models where the state will provide.
Have we learnt from previous 'revolutions', e.g. the Industrial Revolution?	Looking too much at history may not be relevant because the pace of change is vastly different with technological developments and today's world is more interconnected and global. Organisations need to address the change that is coming and work with governments to consider what the future of work looks like and how policy can keep pace with innovation. The public sector will need to support those whose jobs are replaced but needs to be supported with reskilling.
Are we being overly alarmist about this topic when we think back to previous 'revolutions'?	This is different because of the sheer pace of change and the truly global nature of today's world, as mentioned above. Companies cannot just sit back but need to start thinking about the change that is coming, embrace it and work out what to do with it.

Question	*Answer*
If change is happening fast and it is difficult to change huge organisations quickly, will there be more interplay between the different worlds?	Yes – there is likely to be a world that dominates with interplays into others. It will not just be about money but the overall deal and a contingent workforce will still need to represent an organisation's values.
What is the likely impact of unchecked change?	Technology is often a useful tool but humans may be a bad master of it. Organisations need to become better at 'failing fast' or stopping innovations when necessary, while recognising that people are more likely to adopt what they help to create. The automation of jobs is not necessarily bad if the freed up capacity is used wisely.
What is the role of government and regulators?	The education system is currently not fit for purpose in parts of the world and organisations are springing up to bridge the gap between the products of the education system and what businesses now need. The question is whose responsibility is this? If nothing happens, the individuals will fall back on the government for support so corporates need to work collaboratively with governments, with business being vocal about what they need from the education system. At the same time, people need to take responsibility for themselves and look to be agile and constantly develop.
What does this all do to career development, e.g. within law firms, there used to be a long-term investment in people to bring them through to partners?	As people entering the workforce today are likely to have 8/9 different jobs, lifelong learning is becoming more critical and adaptability and emotional intelligence are more important. At PwC, we may need to look for partners from outside the organisation as well as inside and will need to be clear on the deal which links back to purpose and values.
The culture of a company is often what organisations are buying when they pay for consultancy work in the blue and green worlds, so how will this operate if the workforce is transient?	Even with a more transient workforce, organisations will look for people who emulate their values. The 'audit' of culture and values is already happening in the FS world and is likely to spread elsewhere. Without a clear articulation of purpose and values, businesses will be less attractive to talent.
Where will people live? Can they choose to be where they want and will urbanisation therefore reverse?	In a blue or green world, cities may spring up around a large organisation. In a yellow world, individuals are likely to choose to live in relevant communities. In a red world, there are may be hot beds of activity, e.g. tech start-ups in San Francisco.
Are humans genetically programmed to adapt as fast as the world is changing and what will this do to mental health?	This is an important issue and a lot of organisations are already picking up on it. The pressure on workers today in a 'permanently on' world is enormous and looking after their employees' mental health needs to be part of an employer's role.

56% ***of survey respondents think governments should take any action needed to protect jobs from automation***

37% ***are worried about automation putting jobs at risk***

70% ***of respondents in a blue world would consider using treatments to enhance their brain and body if this improved employment prospects in the future***

Eight essential emerging technologies

Emerging technologies should be considered as a core part of every company's corporate strategy. Boards need to sort through the noise to make clear-headed decisions about the most relevant technologies that will sustain revenue growth and enhance business operations. However, with the torrent of technological breakthroughs, it is difficult to even begin to make sense of individual technologies.

Technology is evolving so fast that spotting the 'next big thing' when Boards are trying to decide where, when, and what to invest in, or consider what might disrupt their business model, can feel overwhelming.

To help companies focus their efforts, PwC analysed more than 150 emerging technologies to identify the 'Essential Eight'. These are the technologies we believe every organisation must consider. While each company's strategy for how best to exploit them will vary, these eight technologies will have the most significant global impact across industries.

Presenters:

Sheridan Ash
PwC Director leading PwC UK's technology and investments business
sheridan.ash@pwc.com

Elaine Whyte
Leader of PwC UK drones team
elaine.whyte@pwc.com

Jasnam Sidhu
Co-founder of disruption practice in PwC UK
jasnam.s.sidhu@pwc.com

Jeremy Dalton
Leader of PwC UK virtual and augmented reality team
jeremy.dalton@pwc.com

Need to know

- The eight essential emerging technologies are drones, the Internet of Things, blockchain, 3D printing, robotics, artificial intelligence, virtual reality and augmented reality.
- Many of these are rapidly becoming mainstream.
- It is the convergence of these eight technologies that is really powerful with artificial intelligence often the underlying enabler.
- Companies and their Boards should consider how their business might be impacted by tech driven disruption and whether they are well-placed to capitalise on the opportunities.

Context

The session began with some context-setting around how the eight essential emerging technologies had been arrived at. A study applied various lenses to a diverse population of over 150 technologies. These lenses included:

- the technology's relevance to companies and industries
- global reach
- technical viability, including the potential to become mainstream
- market size and growth potential
- the pace of public and private investment in them.

There was also a brief consideration of the key factors driving the take-up of technologies more broadly, as follows:

- **Increased comfort with technology** – everybody is using multiple devices and tools and therefore becoming comfortable with technology more generally
- **Competitive advantage of technology** – companies are finding ways to use these technologies to create value through new products and services
- **Multiplier effect** – the technologies are converging to create a disruption multiplier effect as they are all connected and support each other
- **Globalisation of technology** – for the first time, the developed and developing worlds are creating, collaborating, communicating and consuming on similar technology platforms generating global innovation with emerging countries sometimes leapfrogging older technologies in the developed world
- **Cheaper access to technology** – prices are constantly coming down for connectivity, storage and processing speeds.

The eight essential emerging technologies

Drones

Drones are devices that participate in flight or movement without a pilot. They have the following features:

- remote controlled
- contain mobile technologies
- scalable
- need to comply with regulations.

Drones are agile and rapid to deploy and are already being used in business where there is expansive real estate or major capital projects. They can also be used for survey mapping, asset inventory management, surveillance and transport of goods. Rwanda has been using drones to transport blood to areas of need.

PwC estimates the global market for drone-enabled services to exceed $127bn by 2030 and, in the UK, this could be 2% of GDP. 29m drones are expected to be shipped globally by 2021.

Internet of Things (IoT)

The IoT is defined as the interconnection, via the internet, of devices with computing capability that are able to send and receive data. It will create a huge amount of data but how to exploit this will be a challenge. Key characteristics of IoT are:

- seamless data transfer
- makes 'things' smarter
- creates efficiencies
- enables smart cities.

Much of this is already in use today in areas such as asset tracking, smart metering, predictive maintenance and fleet management. However, there are risks in terms of both cyber security aspects and a shortage of necessary skills.

Industry growth for IoT is expected to be strong with $1.7tn revenue anticipated by 2020 and 20.4bn connected things.

Blockchain

Blockchain permits the exchange of assets with others using technology, without the need for intermediaries as the position is upheld by others on the network. It is:

- a distributed ledger
- immutable and secure
- a peer-to-peer network
- trusted
- and allows the creation of smart contracts.

In practice, existing use cases for blockchain include verifiable ownership (e.g. Dubai and the UK are considering it for property transactions), standardising healthcare records, minimising voter fraud, and loyalty and reward schemes.

The value of the blockchain market is predicted to be $14bn by 2022 and 77% of FinTechs expect to adopt blockchain by 2020.

3D printing

3D printing is the process of creating a three dimensional object by successively printing layers of materials on top of one another until an object is formed. It:

- is an additive process
- can handle a variety of materials (glass, metal, wood, etc.)
- creates complex objects
- saves labour and assembly line costs.

A 3D printer can therefore replace multiple production processes and can print complex and personalised products. Airline nodes have been printed that are 150% stronger than those produced using more traditional manufacturing. The first 3D house has also been printed in the US and this innovation may help to alleviate the housing crisis.

Business case uses already in existence include complex manufacturing, detailed architectural models, production of spare parts and rapid prototyping.

Estimated annual revenue from 3D printing by 2021 is $20bn and 20% of the top 100 consumer goods companies expect to use 3D printing to create custom products by then.

Robotics

Robotics is the combination of engineering and computer science to create, design and operate mechanical devices, i.e. robots. Key features are that robotics:

- has enhanced sensing control and intelligence
- depends heavily on sensors
- can be autonomous or collaborative.

15% of organisations are investing in robotics today to take costs out of processes. Amazon has a 'black out factory' with no humans, Ford is using collaborative robots to fit shock absorbers to Ford Fiestas and there is even a robotic chef programmed to prepare and cook Michelin starred meals.

The robotics market is forecast to be worth $237bn by 2022 and 14m robotics units are expected to be sold by 2019.

Artificial intelligence (AI)

AI is a collective term for computer systems that can sense their environment, think, learn, and take action in response to what they're sensing and their objectives. It is the theory and development of computer systems that exhibit human-like intelligence. The full benefits of AI come about through the convergence with other emerging technologies where it is often the enabler.

AI is an umbrella term and encompasses a range of technologies including:

- natural language processing
- machine learning
- deep learning
- speech recognition
- machine vision.

By 2030, the global impact of AI on GDP is anticipated to be $15.7tn with the consumption contribution of this being 60% (largely due to greater personalisation) and the productivity contribution 40%.

Practical uses already in existence include autonomous vehicles, healthcare diagnosis, fraud detection within financial services and demand prediction in retail.

Virtual reality (VR)/Augmented reality (AR)

VR is often used as a catch-all phrase for headset and mobile based virtual and mixed virtual worlds. There are in fact three types of immersive technologies:

- Virtual Reality (VR) – VR is the use of computing technology to create an immersive simulated environment, usually through a head mounted display.
- Augmented/Mixed Reality(AR/MR) – AR is the use of computing technology to superimpose virtual images on the user's view of the real world. MR goes one step further by enabling digital and real-world objects to interact.
- 360^0 Interactive – 360^0 videos capture an environment from a single point using actual photos rather than something which is computer generated. The upside is that a realistic environment can be rapidly produced and edited.

8 of the top 10 technology companies have invested significant time and money in VR, including Apple which is not known as a first mover but excels in taking technology and developing it better than its competitors.

Business uses include 'try before you buy', e.g. clothes, touring properties before they are built, prototyping and training.

Industry growth for VR/AR is expected to be strong with $494.6bn global spend anticipated by 2023.

Timing of widespread implementation of these technologies

In terms of the timing, two Gartner Hype Cycles from 2014 to 2017 were compared.

Gartner's Hype Cycle is a graphical depiction of a common pattern that arises with each new technology or other innovation. Each year, Gartner creates more than 90 Hype Cycles in various domains as a way for clients to track technology maturity and future potential. The five phases in the Hype Cycle are:

- **Technology trigger** – where an innovation is identified that could be disruptive
- **Peak of inflated expectations** – where the innovation is hyped up by the media and others in terms of what it could achieve
- **Trough of disillusionment** – where interest wanes as experiments and implementation fail to deliver
- **Slope of enlightenment** – where the use case becomes more mature
- **Plateau of productivity** – where mainstream adoption of the technology takes off and it effectively becomes business as usual.

Comparing the Hype Cycles from 2014 and 2017 enabled an overview of how quickly various technologies were progressing.

Convergence of technologies

The real power of these eight essential emerging technologies comes from their convergence. This drives the speed of innovation and the pace of change. Much of what has been talked about is already in existence and not far from becoming mainstream. In all instances, however, data underpins everything and this is where the competitive advantage will be realised.

A virtual reality experience was used to demonstrate the convergence of these technologies in practice.

Questions for NEDs and their Boards

NEDs should reflect on the following key questions:

- Do you understand how your business may be impacted by tech driven disruption?
- Does your business have the right people, data and technology to help you understand and capitalise on tech opportunities?
- Do you feel equipped to challenge obstacles in your culture that prevent innovation?

Open forum Q&A

Questions that arose in the open forum Q&A covered the following areas:

Question	*Answer*
What is the cyber security risk of all of these technologies?	This does need to be mitigated, using both humans and technology, and there will always be a need to assess on a case by case basis whether the risks outweigh the anticipated benefits.
Is this not likely to happen even faster than we are predicting?	Possibly – all businesses need to be open to the opportunities these technologies bring and embrace them where appropriate.
India, China and Estonia all have national databases being introduced. Is this likely to become part of being a citizen in the UK?	It is possible that existing systems/databases may be joined up or there may be a new database where all data 'from the cradle to the grave' is stored. Data will be a key source of competitive advantage.

77% ***of FinTechs expect to adopt blockchain by 2020***

14m ***robotics units are expected to be sold by 2019***

8 ***of the top 10 technology companies have invested significantly in AI***

China's Belt and Road Initiative and the implications for business

Formerly known as One Belt, One Road, China's much vaunted Belt and Road Initiative (BRI) is a vast, interconnected infrastructure and related ecosystem project, notable not only for its scale but also its timeframe.

The BRI is focused on developing new economies around the world and fostering global trade among them, not just with China. It could therefore spark a 21st Century expansion of global economic growth, technology exchange and, inevitably, Chinese influence.

Presenters:

Suwei Jiang
PwC UK partner
suwei.jiang@uk.pwc.com

David Wijeratne
PwC Singapore partner
david.wijeratne@sg.pwc.com

Need to know

- BRI is possibly the largest trans-continental infrastructure programme the world has ever known and it is just the beginning.
- BRI has the potential not only to develop the much-needed infrastructure but also to facilitate the economic journey of more than 60 countries.
- BRI brings with it a unique set of considerations to evaluate – manifested in the regulatory framework, financing and operational aspects.
- To succeed in delivery, companies should be proactive in establishing contingency plans, build strong and respected relationships and consider better risk sharing.

Definition and context

The session began with some context-setting, explaining what the BRI is:

- The Belt – the Silk Road Economic Belt, i.e. the Eurasia land bridge to Europe
- The Road – the 21st Century maritime Silk Road
- The initiative – to build the ancient land network that connects China to Europe via Central Asia through large infrastructure projects and then to develop an infrastructure ecosystem around these in a massive global connectivity plan.

Six economic corridors are being identified within this via important strategic countries. Arguably the UK is currently at the western end of the BRI as a train route from Yiwu to Barking opened in 2017. This is significantly shorter than the sea journey and therefore reduces costs. Liverpool may also become strategically important going forward as China has been investing in Norway and Iceland given that the Artic Circle shipping route is now open for much of the year due to global warming. It is estimated that this alternative sea route could save China $4trillion per annum.

Officially, the BRI was announced in October 2013 but it has been going on for many decades.

The scale of the BRI is unprecedented involving:

- 65 countries initially and quickly growing to 120+
- 1/3 of the global economy
- 4.4billion of the population and rising.

Around the world, pieces are being put in place – rather like in the board game Go – to be connected later.

BRI goals

BRI addresses industrial overcapacity, currency internationalisation and allows China to gain global recognition. Its primary goals are to:

- internationalise currency and diversify currency risks
- address the surplus in industrial capacity
- be a part of China's economic reform
- increase exports and facilitate trade
- establish global infrastructure capability
- enhance geopolitical relations.

Parts of western China are still very underdeveloped and the aim is to bring these up to the level of the coastal cities. There is also a desire to shift the current sectoral focus in the coastal cities. The aim is therefore a rebalancing of the Chinese economy whilst also connecting the rest of the world with China. Developing countries will benefit from the investment and the ruling party is encouraging Chinese companies to go global without sticking to the traditional countries of the West. The US is currently not included in the plans although some South American countries are now being approached.

The first five years of the current presidency were very much focused on a domestic agenda whilst building blocks, such as tackling corruption, were put in place. In October, a move to focus internationally became part of the constitution. Along with the removal of the term period for the president, there was a realignment of the Cabinet with this agenda, including a department dedicated to BRI.

Opportunities for foreign companies

The first wave of BRI projects are to do with infrastructure whilst the second wave will be the ecosystems around these and the third will be e-commerce. Projects tend to be strategic (e.g. routes through Pakistan providing direct links to the Indian Ocean), commercial (e.g. the port of Trieste which is something in which the Chinese have deep capability) or capability enhancing (e.g. China looking to develop certain technologies such as nuclear power).

In the 1980s, China's approach was more commodity focused but, now that it is based on infrastructure and the accompanying ecosystems, it is looking for partners as it does not have all the necessary capabilities or funding. Companies should therefore consider their China strategy and particularly assess how to work with China outside of China as this is different to operating within the country.

Key opportunities are likely to come from:

- investment of assets
- partnerships in engineering, procurement and construction
- international project management
- supplying raw materials or equipment
- operation of assets
- divestments of assets.

The multi-decade BRI project involves significant investment and China has confirmed it will not achieve this on its own. Many organisations are already taking advantage of the opportunities including:

- **Amec** – providing project management skills as China has no experience of areas such as unions
- **Deutsche Bank/Standard Chartered** – providing financing
- **Caterpillar** – supplying equipment
- **Port of Rotterdam** – operating ports
- **Air France** – divesting certain routes to China.

Many more examples were provided as takeaways.

Opportunities apply across all industries. Key sectors in the early phases are likely to be:

- banking
- financial services
- legal and professional services
- advanced manufacturing
- infrastructure planning
- infrastructure development
- energy
- digital

but, as the ecosystems develop, other sectors such as healthcare, education and tourism will come into play.

Digital is an important element of the plan with many developing countries leapfrogging traditional technologies and going straight to mobile/digital solutions. Being green is also a key aim.

Positioning for success

Although the BRI gives rise to many opportunities, taking advantage of these will bring challenges not just at company level but also at a country level. The UK needs to assess its unique selling point and decide which of the 65 (or later 120+) countries to prioritise. This may be the commonwealth countries where there is similar rule of law and where the UK has knowledge as well as trusted relationships with local partners. France and Germany are already doing this, e.g. France is focusing on the French speaking nations in Africa.

Critical steps for positioning for success are to:

- evaluate not only the specific BRI project but also the maturity of the economic corridor
- evaluate supporting facilities
- consider how each project fits with the company's portfolio
- develop contingency strategies
- establish trusted partnerships
- share the risks.

Any strategy will need to be flexible as China is looking to learn and it is likely that its needs will change as the BRI progresses. The City of London is currently focused on the opportunities in terms of funding with a BRI office headed by Douglas Flint. Theresa May came close to signing a BRI partnership while in China in January.

This is a global competition that is not going to go away and the level of awareness among the UK business community is currently low. There needs to be a proper evaluation process as there are exciting opportunities but the challenges should not be underestimated and it takes time to build trusted relationships with China.

Questions for Boards

Final questions for Boards to consider are:

- How much does your Board know about the BRI?
- Has there been a strategic evaluation of the potential opportunities that BRI presents for your company?
- What are your competitors doing on BRI?
- What further support is needed to help your Board and company to successfully take advantage of the potential opportunities from BRI?

Open forum Q&A

The open forum Q&A was wide-ranging and covered the following areas:

Question	Answer
How set is the route?	The existing routes with the six primary economic corridors are set but there are likely to be further developments going forward.
Where does aviation fit into this?	Ports and roads are still widely used but airports will also come into play, particularly for tourism, and are already being planned in BRI countries.
Is infrastructure still as relevant with technological developments such as 3D printing?	Infrastructure still serves as a cornerstone for ecosystems, e.g. a port leads to a town which in turn needs healthcare and education. However, technology is not being overlooked with Npower putting miles of cable down whilst also exploring Cloud solutions. As noted above, some countries such as Africa have gone straight to mobile, bypassing landlines. China is good at building application technology but is not always as strong in core technology.
What about the relationship between China and India?	There have been geopolitical and border issues in the past. However, both China and India are the world's most populous countries. India will probably need to get involved otherwise China will just go round it. At the same time, China is likely to need access to India's market.

Question	*Answer*
Although there seems to be a 'greying out'/exclusion of the US, aren't some large US companies already engaging?	Despite political views, the US stands to benefit from the enhanced trade. Global companies originating in the US are likely to continue doing business with China but some US companies are becoming very domestically focused and ignoring BRI.
From a geopolitical standpoint, how is this being viewed in Russia, Washington and Delhi?	Fundamentally, China is trying to create commercial markets. It is a very mercantile plan rather than being about 'land grabs'. There are still 600m people in China who need to be lifted out of poverty.
How is this viewed within China – is there a desire to safeguard the current system or is there an opening up?	BRI is commercially focused and is about rebalancing industry sectors as well as having routes through western China to open up trade with the rest of the world. By putting this in the constitution, it has become 'law' and so Chinese companies have to get involved. State Owned Enterprises are no longer domestically focused and are being encouraged to go global but they do not necessarily have all the required capabilities.
Why do developing countries see this as a win-win given experiences with Africa twenty years ago?	Previous experience was much more commodity driven, i.e. getting ore to China as cheaply as possible. There was no real ecosystem but this time the ecosystem around projects is making a difference and China is also involving the local communities. For example, there are now lots of cultural exchanges with Africa. BRI projects that have tried to use the old model have tended to collapse.
How will JV companies be financed?	China will look for external funding of all types, including bank loans, co-investment, specifically raising funds to invest, etc. The City of London is keen on raising green bonds, although there will need to be close monitoring of how the money is used. Dividend flows to JV partners should not be an issue as this is a tried and tested route once the right paper work is in place. BRI projects are generally being given the green light.
Is there a blueprint for funding?	Not yet but this is coming as companies want transparency in order to provide funding. China does not have sufficient funds on its own so needs investment from outside. A new agency is being established to provide clarity and an international think tank has been set up to understand what international companies are looking for. However, how much transparency there will be remains to be seen.
What about the tightly controlled and planned central government approvals?	If there is a need to get money out of China, companies will have to go through the foreign currency controls process but, if the funds are already outside of China, the process can be by-passed. As noted above, there is more certainty of approval with BRI projects.
Is there an overall master plan?	Publicly, no but it is likely that there is within central government. Nevertheless, China will need to take cautious steps and probably revise any plan along the way due to the world changing around it.
Is this an opportunity for China to take control of standards and engage in extensive data collection?	There is more likely to be convergence rather than China laying down standards. The FCO is already working with China to seek more convergence in areas such as the rule of law, low carbon emissions, financial services, etc. and the UK is not alone in trying to influence this.

Question	Answer
Given the capability gap, will China show greater respect for Intellectual Property (IP)?	As noted above, standards and rules are a key discussion point at government level. China's strategy has to change as it needs overseas partnerships and taking IP would be very short-term as the partner would not work with China again. In addition, some Chinese companies such as Ali Baba are now worrying about their own IP which has changed the climate. IP can be used an excuse for companies not to get involved with China but SMEs seem to be less concerned than larger companies. They take an approach of 'what can we create and come together to commercialise' rather than 'what are we going to lose'. China provides the scale for these innovative companies to grow.
Is 'soft power' part of the mix, as it was previously in America?	Yes, as hard economic power will not be enough on its own. There are many cultural exchanges and other sharing of experiences in education and healthcare. China is also trying to involve countries such as Africa in this.
Is it true that the BRI is about exporting China's carbon footprint and pollution?	Being green is a key theme of the BRI. However, it is definitely about exporting excess capacity.
Is there concern about the other countries involved in BRI becoming competitors?	Not really as, other than India, not many have the scale of China. China is already positioning itself as a 'senior states-person' in relation to countries such as Vietnam and Cambodia.
How does the very long term plan fit with China's demographics?	Getting more people into employment, rebalancing the industry sectors and seeking to improve society within China is all part of the master plan.
What could make this fail?	A fundamental risk would be the stability of China, as it hinges on a stable government, hence the recent presidential term removal as part of this.
The BRI has had little profile in the UK and some companies have had poor experiences with China in the past but presumably there will be an impact on companies who ignore this?	It is a competitive environment and Germany is already very focused on this as Chinese/German relations have always been better. Education and awareness in the UK are definitely an issue. The UK sent a strong delegation to the BRI summit hosted in China last year but there was almost no media coverage of this in the UK whereas it was front page news and reported very positively in Germany. This disconnect in the UK media may in part be because everyone is consumed by Brexit but also possibly because there can be a tendency to look for the sensational and report negatively. The media is not currently helping business to understand that the landscape and climate in China have changed.

65 *countries in initial plans growing rapidly to 120+*

1/3 *of the global economy*

4.4bn *of the population and rising*

Delivering total deal value

In today's complex and challenging business landscape, M&A can be one of the most effective ways to build value for an organisation. However, done badly, it can lead to significant loss of value. NEDs can play a critical role in influencing the value creation agenda, by ensuring the appropriate depth of planning takes place at the start, that the transaction execution is appropriately managed and overseen, and in holding leadership to account in delivering and securing value for the company.

The session aimed to explore how M&A can create value and where it might not, as well as discussing the role of NEDs in M&A, including typical level of involvement and influencing the value agenda.

Presenters:

Hein Marais – Head of value creation in deals
hein.marais@pwc.com

Nick George – Strategy partner
nicholas.d.george@pwc.com

Simon Harris – Valuations director
simon.harris@pwc.com

Abhi Shah – Deal value architect
abhi.shah@pwc.com

Mark Wood – Chairman of Nominet and PwC Advisory Board member

Need to know

- Growth strategies driven by acquisitions can be highly effective if there is a proper value blueprint in place.
- It can be helpful to think of a deal in three key phases – value identification, M&A execution and value realisation.
- Looking at individual value levers in the areas of improving strategic positioning, optimising performance and optimising tax and the balance sheet, which together combine to drive multiple uplifts, can help to ensure value is maximised.
- Fairness opinions can be a helpful tool in testing the value proposition of a transaction.

Introduction

The session began with three key questions that should be asked regarding any deal:

- Does this deal fit with our strategic rationale and long-term vision?
- Is the business valued appropriately?
- Is now the right time?

Further considerations should include:

- Who is responsible for delivering the value after the deal is done?
- Is there a value blueprint in place to ensure maximum returns?
- How is this deal helping to future-proof our business?
- Do our people really have a value creation mind-set?

EBITDA multiples have increased by 30% and so shareholders' expectations are definitely rising.

A NED in the room agreed that the above were key questions and noted that it is also important to create an anchorage of agreed terms and expectations for the deal at the outset so that these can be returned to as the deal progresses and the executive team get swept along in the excitement.

It was also suggested that many M&A deals these days are to gain access to technological innovation or acquire skills.

Initial research findings

The initial findings of some research conducted by PwC in conjunction with Mergermarket, looking at company performance following an acquisition or divestment over the economic cycle from 2008-2016, were presented. This research will be overlaid with more than 200 1-to-1 interviews and is due for publication in October.

Initial findings suggest that:

- Growth strategies driven by acquisitions can be highly effective with a 5% uplift on average over a 12 month period.
- Acquisitions offer the potential for significant outperformance on the upside.
- Significant outperformance versus the norm is possible in periods of greatest change as the 2009 class of acquisitions had yielded the strongest performance.
- Tech, media, telecoms and industrial products and services show the strongest average returns performance from acquisitions. However, there was less variation between industries than might have been expected.

In terms of divestments, preliminary findings suggest:

- Divestments remain a challenge as the performance of divesting companies was worse than peer group and other comparators.
- This negative performance appears to worsen over time.
- The upside potential on divestments appears to be capped, unlike acquisitions.
- Divestments can improve performance in periods of stress as 2009 was again a good year.
- Divestments often appeared to be a 'sign of weakness' across all industries.

The implications of these findings are that:

- there may be uncertainty over 'what good looks like' in outcomes on acquisition performance, with a temptation for short-termism and focusing on the easy wins such as cost cutting, rather than building for growth
- the rationale for divestments is not being well-articulated and the actual execution of the divestment is also not being done well, with it often being difficult to draw the line and move on
- executive turnover and loss of key talent may occur
- failure to maximise the opportunity for true transformation can result.

NED perspectives

One of the NEDs present talked about a company that he became Chairman of as it was in the process of making an acquisition. A competing bid had emerged and the price had gone up but the company still wanted to close the deal as a lot of work had been done at that stage and there were not many alternative deals out there.

There had been clear parameters for the deal at the outset but the company had moved away from these. The NEDs felt uncomfortable about this and in the end the deal did not proceed. With hindsight, the executive team recognised that it would have been a strain on the business had the deal gone ahead and were glad that the NEDs had stood firm.

In another example, where there was an approach to buy a part of the business, it took three years to obtain the figure the business had been valued at but the NEDs stood firm until that price was reached, despite the acquirer cajoling individual Board members.

Key stages in valuation across the M&A lifecycle

It can be helpful to think about the key stages in valuation across the M&A lifecycle in three phases – Value identification (pre M&A), M&A Execution, Value realisation (post M&A).

Often there is a great deal of focus on the middle phase of getting the deal done but less on the value identification and value realisation phases.

Questions that can be considered in each of these three phases are as follows:

Value identification

- What are the strategic options and how will they impact the portfolio strategy?
- What is the long-term value creation plan?
- Is a transaction blueprint in place?

M&A execution

- Who is leading the due diligence?
- Will a fairness opinion be completed and is the adviser independent?
- Who will engage in the negotiation?

Value realisation

- How to take control?
- How to deliver value?
- How to implement operational change?

A 'value bridge' model was discussed, illustrating the different levers that can be used to drive value in the four key areas of:

- improving strategic positioning
- optimising performance
- optimising tax and the balance sheet
- multiple uplift.

It is effectively the first three of these that drive the multiple uplift. Often companies who have made an acquisition focus particularly on optimising performance but sometimes overlook the value levers in the other areas.

However, it is important to recognise that companies do not just need a comprehensive plan but also need to be out in the market talking about it to investors.

An NED suggested that the model focused too much on outcomes and that areas such as customer focus and long-term employee engagement are extremely important these days. It was agreed that the model is a simplified tool and that culture is vitally important and needs to be kept in mind as a key enabler. Nevertheless, the model can be helpful in discussions with the executive team and subsequently in holding them to account.

Fairness opinions

Fairness opinions are a tool to test the value proposition of a transaction. They are often commissioned when a deal is on the cusp of being value accretive or where the deal is very complex.

In the US where there is a higher risk of shareholder litigation around deals, fairness opinions can offer a degree of protection. In Canada, an acquisition had been blocked due to insufficient detail in the fairness opinion and because the adviser had been incentivised on the deal going through. The ICAEW in the UK has picked up on this and issued comments around compensation arrangements and governance shortcomings.

Increased disclosure around fairness opinions is likely to cover:

- guidance that advisers' compensation arrangements should be disclosed
- more impetus on Boards to explain how they took such compensation arrangements into account when approving transactions
- disclosure of other relationships with the financial adviser
- a clear summary of the methodology behind the opinion
- explaining the relevance of the fairness opinion in determining the recommendation to proceed with the transaction.

Independent fairness opinions can be a sign of strong governance, provide more transparency and limit downside.

Questions for NEDs and their Boards

In a transaction scenario, NEDs should reflect on the following key questions:

- Is this deal really transformative or just an add-on (transformative deals pose different and more challenging questions)?
- Is there a 'value blueprint' (detailed value creation plan) in place?
- Is accountability end-to-end across the transaction lifecycle clearly assigned (not just accountability for doing the deal)?
- Is the company drawing on all available sources of expertise and consulting?

Open forum Q&A

Questions that arose in the open forum Q&A covered the following areas:

Question	*Answer*
How did the NEDs challenge the deal in the example presented, given the strong bias of the executive team, and is there anything they would have done differently with hindsight?	The outgoing Chair had indicated that the deal had moved away from the initial parameters so the NED first raised this with the CFO and a couple of other executives. It later became clear through discussions with other Non-Executives that they were also feeling uncomfortable as the deal had moved so far from the initial parameters and this provided the impetus to go back to the executive team and stand firm.
Is it possible to expand on the preliminary research indicating an average uplift in value of 5% over a 12 month period following an acquisition, as many deals still seem to fail to deliver the anticipated returns?	There are still probably as many deals that don't add value as do but the 5% uplift is an average. Technology change has been driving more value. Synergies have often been delivered as a result of deals but business as usual has suffered.
What is the definition of value as this can come through at many different levels, e.g. Nestle's deal to sell Starbucks coffee brands was to do with strategic positioning?	It is important to look at a deal in terms of its many facets and not just EBITDA. Every organisation will have a different perception of value and the value plan therefore needs to be bespoke to the company. It is also important that once the value proposition has been defined, it is clearly articulated to shareholders.
In what percentage of fairness opinions has PwC said that a deal is not fair as some cynicism exists at Boards about the value of these where there are caveats about relying on the commercial views of the Board?	Often the terms of a deal have been tweaked following a fairness opinion.
The four concluding questions are very sensible, even outside of an M&A situation – how would they change if the company was being acquired rather than acquiring?	Often management and the Board are caught off guard in a hostile takeover situation. They need to be more prepared to communicate the long-term value of an organisation to the market and NEDs therefore need to ensure they have sufficient information to understand the company's true value. It is incumbent on the NEDs to keep the executive team honest.
There should be a piece around the NEDs' involvement in deal picking – where is this?	This is not seen enough in practice. However, having a diverse group of NEDs who can evaluate alternative deal targets and report back to the Board (with expert support where necessary) would be a good policy.
How important are people and culture in a deal?	Deals often fail because of cultural issues and it is important to work out whether any potential clash is likely to be insurmountable. Assessing culture may depend on the level of access as it is helpful to talk to people (not just the top management but also, for example, the key sales people) and sometimes use can be made of AI. It may also be possible to get a view of the culture based on the decision-making process. Some acquisitions are in fact made to bring in strong management teams.

Rethinking reputational risk

Reputations take a long time to build but can be destroyed in an instant, particularly in today's social media driven world. However, reputation is widely recognised as important as companies and their Boards will be well aware in the light of certain recent high profile failures.

Whilst the direct causes of crises are often people sitting in the lower half of the hierarchy, root causes are more often found among systems and the leaders at the highest level who drive and supervise them.

Reputational risk can be defined as the risk of failing to fulfil the expectations of stakeholders in terms of performance (what you do) and behaviour (how you do it).

So why do seemingly well-respected organisations unexpectedly fail? It has taken a long time and the analysis of scores of case studies to unravel this but the answer is now clear. This session was an opportunity to cover:

- ***the nature of reputation and reputational risk***
- ***why the seemingly sound catastrophically collapse***
- ***what drives reputational risk – the role of human behaviour***
- ***why these drivers are hard to find***
- ***the crucial role of leaders, especially Chairs.***

Speakers:

Anthony Fitzsimmons – Chair of Reputability LLP, lead author of *'Rethinking Reputational Risk: How to manage the risks that can ruin your business, your reputation and you'* and an authority on reputational risk and the behavioural, organisational and leadership risks that underlie it.

Need to know

- Organisational failures are not usually caused by bad people, they are caused by systems failures.
- Since organisational systems depend on people, systems failures depend on how people are organised.
- Since organisations' systems are designed, run and led by leaders, it is leaders who are thus, unwittingly, often the root causes of failures.
- After a crisis, Boards are regularly shocked to discover what has been going on. This is a problem for all of humanity – we are blind to our blind spots, a phenomenon well understood by psychologists.
- Leaders' character is much more important in these failures than is recognised, as is their skill, knowledge and experience both in life and in work.
- Leadership from the Chair is essential in tackling these risks because their root causes are usually found in or near the Board.

Introduction

As a lawyer specialising in liability, risk and insurance, Anthony had three decades with a ringside view of things going wrong. Later he was co-author of *'Roads to Ruin'*, the seminal Cass Business School report for Airmic, which uncovered many of the widespread but hitherto unrecognised reasons for failure through a study of 18 substantial corporate failures.

'Rethinking Reputational Risk: *How to manage the risks that can ruin your business, your reputation and you'*, the recent book co-authored by Anthony, analyses these causes systematically and answers the question: 'Why do seemingly sound companies fail?' before explaining how leaders, and only leaders, can bring these risks under control.

Context

Reputational risk is a huge issue because a lost reputation costs shareholders a great deal as well as undermining the organisation's ability to earn and raise money.

The problem with most crisis post-mortems is that they do not dig deep enough. They tend to dig to the 'proximate cause' beloved of lawyers and judges rather than to deeper systemic and root causes, as the aviation industry does. The result is that someone who made a mistake gets blamed without considering whether, or why, the system in which they were operating drove them to it.

For example, if a company overstates its profits, clearly someone put the accounts together that way. But why? It might have been direct pressure from their superior or the perceived wish of their superior (my boss's bonus and/or self-esteem depends on stretching profits). Those in turn might be the result of culture or of recruitment and remuneration practices (for example paying insufficient attention to character in recruiting leaders and adopting incentive schemes that encourage undesirable behaviour), all of which may stem from skill gaps at Board level, such as insights from psychology and sociology.

What are 'Reputation' and 'Reputational risk'

Your reputation is the sum total of how your stakeholders perceive you. Reputation is about perception.

Many corollaries follow from this deceptively simple definition. One is that you lose your reputation when your stakeholders come to believe (rightly or wrongly) that you are not as good as they thought you were.

From this flows a robust definition of reputational risk: the risk of failing to fulfil the expectations of your stakeholders in terms of performance and behaviour. Performance is about what you do and behaviour is about how you do it. Again this is about perceptions.

Key insights

Anthony presented a series of key learnings that have come out of the many years of study of corporate failures. An early observation from scores of case studies is that:

1. Organisational failures are usually caused by bad systems, not bad people

This is not to say that bad people never cause crises but when a person is judged to be 'bad', it is rare to find that they are intrinsically bad. Digging more deeply, it is common to find that a normally decent person was incrementally encouraged, by the organisation's incentives and culture, to start doing things at the margins between good and bad before being nudged over the edge.

These systems can be divided into:

- front-line systems that deliver what the organisation is about, (for example delivering cars, audits, legal opinions)
- underlying systems (e.g. IT systems) and
- people systems that help the entity's people to cohere.

However, in reality both front-line and underlying systems depend on people, so:

2. Organisational failures are ultimately about failures in the way that people systems are organised

What do causes of organisational failures look like below Board level? They have to do with:

- how the organisation recruits, rewards and promotes its people
- incentives, financial and behavioural
- poor examples from superiors
- culture
- ineffective communication – a common symptom is that bad news travels upwards less fast than good news
- failure to listen – people may not listen at all or they may interpret what they are told to fit their world view
- risks from internal and external complexity
- risks from poor change management
- long incubation periods making it easy to misallocate causes to consequences
- complacency, reinforced because we don't recognise the roles of luck and system failures when we overcome minor mishaps.

Virtually none of the associated risks are captured by classical risk management which means there is also a hole in the 'three lines of defence'. Almost of these are systemic risks that, at their roots, ultimately emanate from the decisions, behaviour and character of leaders. Thus:

3. Leaders are ultimately responsible for the design and management of their organisation's systems, including people systems, which means that leaders are important causes of failures

People systems have many aspects but any people system will be dysfunctional if it doesn't learn from errors or if it lacks reliable effective communication. Neither is possible without good leadership.

Every leader readily accepts that they have the power to achieve great things. However, most leaders seem to find it hard to accept the logical corollary – that great power also brings with it the ability to cause disastrous outcomes when they err. Psychologists see this as an example of self-serving bias – we attribute success to our skill and failure to outside forces or bad luck.

What aspects of leaders cause their systems to fail? It is rarely a lack of intelligence, though the 'cult of the gifted amateur' has much to answer for. Gaps in skill, knowledge, experience and perspective are far more important than people believe. Without them the NED team cannot challenge or support executives effectively. This is not to suggest that gender and BAME diversity are not important social justice issues.

The personal ethos and character of directors also matter – for example, NEDs who lack courage won't challenge when they should. So too do a host of other leadership characteristics, such as:

- hubris, bombast, arrogance, greed and complacency
- C-suite incentives
- perceived behaviour and wishes of leaders
- leaders' inability to receive or absorb dissonant information
- collegiality – comfortable but dangerous, easily leading to Groupthink
- ignorance of how cognitive biases and social behaviours subvert discussions and decision-making
- lack of self-awareness.

Once again these risks are not covered by classical risk management, enlarging the hole in the 'three lines of defence' through which most modern reputational crises slip. Unfortunately the self-serving, overconfidence and optimistic biases doom attempts at internal self-evaluation to be ineffective. Few, if any, external Board effectiveness evaluations appear to be effective in finding, let alone dealing with, these risk areas.

4. 'Leadership on Trial'

The importance of character in business leadership seems to have been neglected until recently. *'Leadership on trial'* (2010) is an excellent report by the Ivey Business School which put this right. It provides two important insights into the role of character in leaders.

The first is that skills, knowledge and experience affect what leaders can do but character determines what leaders will do. Thus, for example, a cautious CEO is more likely to take decisions that reduce risk whereas an arrogant one will tend to listen less to warnings about risk.

The Ivey School also provides a practical approach to dealing with character traits at Board level. Boards that understand the importance of character will hesitate before taking on an aggressive or arrogant CEO. Nor is one well-endowed with patience, caution or humility a comfortable choice.

The Ivey School's second insight is that pairs of potentially undesirable traits can be desirable. Thus a CEO who balances drive, even aggression, with patience is much more desirable than one with one trait but not the other. Similarly a self-confident or arrogant CEO can be dangerous, particularly if the self-confidence is a veneer that disguises insecurity. But a CEO who is sufficiently self-confident to have the humility to welcome, absorb and act on criticism and challenge is a different proposition.

5. We are blind to our blindness

Our lack of self-awareness has another important consequence – we (including teams such as Boards) cannot reliably see our own weaknesses.

To make things worse, our blindness to our own weaknesses is wired into human psychology by biases and reinforced by well-recognised social behaviours. As Nobel laureate Daniel Kahneman wrote,

'We're blind to our blindness. We have very little idea of how little we know. We're not designed to know how little we know.'

This is why Board self-evaluation is likely to miss a Board's most important weaknesses. Only external evaluations can find these, and then only if the evaluator understands the real root causes of Board failures.

6. Complacency kills

Most Chairs rightly fear a reputational crisis – yet our cognitive biases make us complacent and steer us to believe that bad things only happen to other people. Overcoming this delusion is a Chair's first task.

From there, the good news is that the incubation period of most crises means that Boards probably have time to find and start fixing the systemic risks before they cause harm. That said, there is no time to procrastinate as procrastination also increases the reputational risks.

7. Leadership

Who should take charge? The biggest systemic risks emanate from the Board and the C-suite. This means that only the Chair can take overall responsibility for reputational risk and its behavioural, organisational and leadership risk drivers. Clearly there will be some delegation but this must be done recognising that no person should be made responsible for dealing with risks that come from their own level or above.

Thus the CEO should be responsible for these risks below the C-suite but the Chair must be responsible for them in the C-suite and Board. The SID should take charge of risks from the Chair.

8. Crisis prevention is important

Most leaders believe that since the 'three lines of defence' underpinned by good risk management take care of all significant risks, what remains to avoiding a bad crisis is crisis preparation and effective crisis management.

Sadly this widespread belief is wrong because classical risk management does not deal with the behavioural, organisational and leadership risks that are so frequently the cause of reputational crises. As a result, the 'three lines of defence' inevitably has the same hole. This is the hole through which most modern reputational crises emerge.

Crisis preparation and effective crisis management do matter but by tackling the behavioural, organisational and leadership risks that are the root causes of most reputational crises, reputational crises can prevented.

Open forum Q&A

Questions that arose in the open forum Q&A covered the following areas.

Question	*Answer*
Why does a crisis often come as a shock?	Most successful people tend to believe that bad things 'will not happen to us' – overconfidence, optimism and self-serving biases are at work. However, if people are conscious of their biases, they can try to overcome them. Another phenomenon is 'social silences' where everybody may be thinking the same thing yet nobody mentions it because our social behaviours tend to leave most of us wired to conform to the group we are in. However, it only takes one person to break the taboo for others to say they had the same thought. Biases may be further reinforced by people recruiting in their own image. For example 80% of FTSE100 Board members are either Chartered Accountants or come from the C-Suite.
Does diversity reduce crises as there still seem to be as many?	This is not really about the social justice issue of gender/ethnic etc. diversity. If the women/minorities joining Boards have similar backgrounds to the men, the only change is a gender/ethnic-driven change of perspective. The diversity that is key is diversity of skills, knowledge, experience and perspective. A lack of this kind of diversity is regularly the downfall of Boards.
What about the long-term view versus short-termism and is there danger in not taking a long-term view?	Encouraged by politicians, the FRC's latest consultation recommends taking a long term view and this is undoubtedly beneficial to company health. Too often, companies (sometimes driven by investors) cut maintenance and investment to boost profit today at the expense of tomorrow. Arie de Geus called it 'sucking a puddle dry' rather than 'keeping the river flowing'. As an example of the latter, Shell began thinking about life after oil in the 1970s. It would be helpful if the incentive period of bonuses extended well beyond the tenure of a CEO. [See note at end regarding what the FRC has decided.]
If humans are hard-wired to think this won't happen to them, can this be offset?	We can override our biases by being actively conscious of them, although to do so takes considerable mental energy. It also needs someone on the Board who really understands how people operate at the psychological level. Research has left Anthony convinced that every Board should have a NED who understands psychology and social behaviour.
Is dealing with reputational risk the Chair's job or someone else's?	Having looked at this with groups of professionals three times over the past fifteen years, each time the answer has been clear – the Chair has to take overall responsibility for reputational risk.

Question	*Answer*
Is looking at the likelihood of risks also causing risk blindness?	Yes, as seemingly low probability/high impact risks can have a massive reputational impact if they happen but are rarely given enough attention by risk professionals or Boards. The other problem is that if you have a system or underlying state of affairs that is prone to cause a catastrophic failure, a seemingly minor incident can set the system to flip towards catastrophic consequences. A large proportion of big reputational crises seem to be of this kind. Good NEDs will try to get these systemic weaknesses identified and dealt with. Reputational risk can be triggered by surprising, sometimes seemingly minor, incidents and a probability cannot really be assigned to them without understanding the underlying system weakness or state of affairs. You also need to ask about your risk appetite for reputational damage. How much of your reputation can you afford to lose?
The image of the Big 4 is currently suffering from reputational risk – what can be done about this?	Professional firms are struggling with a combination of issues and social media has changed the way matters are perceived and amplified them further. People have views that are communicated instantly. The back story of bad things is instantly available too. The fact that good audits far outweigh bad ones gets forgotten or becomes irrelevant in stakeholders' perceptions and reputation is all about perceptions, not about some objectively balanced view of reality. Rebuilding trust on sustainable foundations is a major task that cannot be achieved until the root causes of the problem have been identified, acknowledged publicly and addressed. This is not a PR job. It is about finding and fixing the fundamentals. This is impossible for leaders to do without robustly analytical and critical but trusted friends because we cannot reliably see our own weaknesses as clearly as we can see weaknesses in others.
Despite increasingly onerous regulation, companies don't seem to be any better at preventing crises – why is this?	The social media frenzy goes a long way towards highlighting and escalating crises in a manner that was not the case in the past. However, perhaps the most important reason is that these risks are not covered by classical risk management, let alone the 'three lines of defence', which leaves them unrecognised and so unmanaged. Most major crises slip through that hole.

Question	*Answer*
Many Boards don't have the capacity to 'think the unthinkable' or don't think it will happen to their Board – any suggestions?	Boards need to begin with consideration of what the organisation's reputation is worth, in both monetary terms and in respect of other advantages it brings, such as licence to operate. From there, setting risk appetite for reputational risk should be a wake-up call regarding the implications of losing that reputation. For most organisations, losing their reputation is destiny-changing. Reputational risk often stems from systemic issues and therefore finding and understanding systemic issues is a good place to start. The flight safety side of the aviation industry has successfully tackled systemic risks by capturing and analysing seemingly minor mishaps to root causes – then fixing the systemic issues. Even a suicidal airline pilot was found to be a systemic issue as patient confidentiality had prohibited the pilot's private doctor from telling the airline that his patient, the pilot, was clinically depressed. So they fixed the issue. When looking at single potentially reputational issues, a useful mental test (courtesy of Warren Buffett) is to consider what your grandmother would think if the issue or behaviour was explained to her in lay terms in her local newspaper.

Afternote on the new FRC Code and Guidance on Board Effectiveness

The FRC has in fact given great prominence to Boards promoting 'long term sustainable success'.

It has also gone out of its way to encourage Remuneration Committees to 'develop formal policies for post-employment shareholding requirements encompassing both unvested and vested shares' forcing executives to hold shares until well after they leave. Since incoming CEOs are already strongly motivated to find any ticking time bombs left by their predecessors, this is likely to be a highly effective way of discouraging CEOs from boosting short term profit at the expense of long term sustainable success.

Blockchain and cryptocurrencies – applications and risks

Blockchain has its origins in Bitcoin and is widely used for cryptocurrencies. It is a relatively new and complex technology that has the potential to disrupt many aspects of business and economies.

Blockchain is a 'distributed ledger technology' which is reliable, verifiable, confidential and secure. The core principles of the technology mean it could impact a vast array of industry sectors and the workshop was an opportunity to explore the application opportunities and associated risks of blockchain and cryptocurrencies.

PwC experts:

Steve Davies
steve.t.davies@pwc.com

Seamus Cushley
seamus.cushley@pwc.com

Need to know

- In today's constantly changing world, trust in institutions has broken down.
- Blockchain enables the establishment of trust between two people, organisations or machines without trusted intermediaries, which enables value exchange.
- Blockchain – a distributed ledger – has the ability to disrupt all transaction processing systems across all sectors.
- Crypto-tokens, including cryptocurrencies, are one application of the blockchain technology.
- Cryptocurrencies may become mainstream as regulation catches up.
- Increased regulation, regulatory enforcement, more institutional players, new business models and innovation are all likely to be trends in the blockchain/cryptocurrency arena going forward.

Context

The workshop began with a look at the context for blockchain which is the current lack of trust in institutions. The fundamental principle of blockchain technology is trust but the technology will only be of interest if it can be used operationally or to encourage growth.

Change is now constant with various megatrends impacting the world, including:

- demographic shifts
- shifts in global economic power
- rapid urbanisation
- resource scarcity and climate change
- technological development.

Of these, technology is both the most disruptive and moving at the fastest pace, with eight essential technologies emerging ahead of the others – virtual reality, drones, blockchain, robots, augmented reality, 3D printing, artificial intelligence and the Internet of Things. Although blockchain may have started out in the Financial Services/Fin Tech world, its centre of gravity is now moving beyond this to many other sectors. Cryptocurrencies are also proliferating, mostly coming out of Asia, and regulation is not keeping up.

Trust

Trust is fundamental to people and business and enables the bridging of the gap between the known and unknown. Technology is creating new ways for people to trust others by providing truth and transparency. In days of old, trust was local and based on a person's reputation. Then trust gradually became institutional to enable global commerce. We are now in a highly connected world where trust has broken down and yet individuals still need to exchange value. **Blockchain enables the establishment of trust between two people, organisations or machines without trusted intermediaries, which enables value exchange.**

An innovation continuum exists from sustaining (e.g the incremental changes made to improve the results of the British cycling team) to the truly disruptive (e.g the invention of the smart phone). Blockchain has the ability to disrupt all transaction processing systems.

Bitcoin is one application of blockchain. As a network, Bitcoin is completely open around the world with anyone able to join and therefore uses a lot of energy. Other closed networks would use less. Although there has been some discussion about Bitcoin being used for criminal activity, this element is relatively small in absolute terms. Activity is tracked and traced on the network and there is in fact greater traceability than with a banknote.

To join a permissioned network, Know Your Client (KYC) and Anti Money Laundering (AML) approval will be requested and there will still be the need for a governance structure. The difference is that it is the actors on the network who set the rules.

The blockchain lens

Put simply, blockchain is:

- A ledger – a blockchain is a way of storing and sharing data between participants
- That is shared – everyone participating has an up to date copy of this ledger
- And where additions are agreed – additions needs to be agreed upon by the majority.

A transaction between two individuals will be broadcast to all on the network in an agreed structure. The consent of others is then needed to validate it. The role of intermediaries that may previously have done this can be hardwired into the rules of the network. It is therefore a centralised governance structure with a decentralised technology system.

The difficulties often come in getting the participants to agree the rules up front and the encryption can also be complex. Blockchain may therefore be used more in a B to B context than B to C, except for examples such as cryptocurrencies. Majority rather than unanimous approval is sought for validation to allow for occasional systems issues experienced by individuals, etc.

Bitcoin is a combination of technologies of which blockchain is one element – the distributed ledger – and was created to prove that there is no need for an intermediary, i.e. a central bank. Nobody has successfully hacked bitcoin to date, although exchanges have been hacked.

A blockchain lens can be applied in four main areas:

Digital currencies

This is where the blockchain technology was born with Bitcoin being a first generation cryptocurrency, although there are now many others such as Ethereum, Ripple, EOS. Other uses can be foreseen such as Insure coin, used in an insurance claim to ensure, for example, that the money is used to pay a mechanic to fix a car. Some large organisations are also looking at having their own internal currency to eliminate exchange differences between group companies.

Digital assets

Here the participant in a network would be able to understand the movement of an asset. This could be helpful for reasons of provenance, e.g. airplane parts or tracking and tracing in mining. If a regulator had 24/7 access to the network, this would change risk discussions.

Identity

This is possibly the key that unlocks most potential, although the network keepers will still have a role to play. There would need to be verification at the point of entry to allow access to the network but then it would be protected thereafter so, for example, KYC digital identity could be shared with different banks. The UK government is currently grappling with what a digital identity might mean. It would require trust in both the gatekeepers and the network.

Smart contracts

Applications could exist in transfer of ownership, or in mortgages and loans, where there is a single source of the latest version. Once the rules have been articulated, process and logic can be applied to the data.

A number of real life proof of concept cases were explored but this has not yet moved to 'industrialisation', although properties are already being exchanged on a blockchain in other parts of the world. As noted earlier, the consensus mechanism for establishing the rules can be difficult to agree and the technology is still in its infancy versus scalability and speed. The sharing of the required information also slows adoption in some instances. In addition, regulatory requirements still need to be met.

As part of the 'industrialisation' process, it is perhaps more likely that there will be a move from the 'boil the ocean' financial services applications to smaller uses in the non-financial services world as experiments to build confidence in the technology.

It is worth noting, however, that the move to execution can be quite simple once the proof of concept has been established and the rules have been set. It took 5-6 weeks to set up a test network for the Bank of England and so the execution period is relatively short once rules have been agreed.

Cryptocurrencies

Blockchain and related technologies provide the potential to drive transformation across numerous business processes in multiple industries, to generate process cost savings worth billions of dollars and to create trust for complex ecosystems. For this reason, Gartner has forecast that, by 2025, blockchain will generate an annual business value of over $175 billion, rising to over $3 trillion by 2030.

There are many different possible uses of blockchain of which crypto-tokens is one. We already live in a world of tokens from gym memberships to season tickets to airmiles and many others. Digital tokens enabled by blockchain could be bought, used, exchanged or sold. The most advanced regulatory thinking in this area is in Hong Kong.

There are four main types of crypto-tokens:

Cryptocurrencies

These are tokens with an attributed value for exchange/transactions, asset/value storage and/or unit of account. Bitcoin was the first but there are now many others. In fact there are more than 3,000 cryptocurrencies on more than 10,000 exchanges. As of 2018, the total market cap of the cryptocurrency market was US$435 billion made up of 37% Bitcoin, 16% Ethereum, 8% Ripple, 2% Litecoin, 1% Dash and 36% other, with Bitcoin down from 86% of the total in March 2015.

Utility tokens

These are digital tokens offering access to a platform and often used for supporting services/functionalities on a blockchain-based platform. Often an ICO white paper describes the concept of what the platform will be used for. This has a utility value and is not a security.

Asset-backed tokens

These are tokens that provide underlying exposure to real world assets (e.g. gold, diamond, cash, real estate, etc.). They can be used to raise money to mine gold, for example, or to trade gold on markets.

Security tokens

These are tokens that intentionally have security characteristics, e.g. debt, equity or derivatives with an income generating component or potential rights vis a vis the issuer.

Crypto-tokens are, however, causing concern for the following reasons:

- Token hybrids – tokens can morph across the four categories described above and are not always clear
- Speed of innovation – the regulators are on the back foot, although they are further advanced in Asia
- Complexity – they are difficult to understand, e.g. use, storage, etc.
- Libertarian paradigm – some projects have the intention of removing intermediaries and putting trust back in the hands of the consumer
- Criminality and fraud – concerns over where the money goes and whether it is fraudulent
- Speculation, hype and volatility – for example, the price of Bitcoin has ranged from £20,000 to £6,000.

Initial Coin Offerings (ICOs) are a limited period in which a company offers a pre-defined number of crypto tokens to purchasers/investors. US$5,961m has already been raised in the first quarter of 2018 across a wide range of sectors. Often the white papers produced in support of the ICO are very thin. For example, Blockdot1 talked about trying to build a more energy efficient blockchain platform and its white paper did not provide many details nor did the ICO grant participation rights. Nevertheless, this ICO still raised US$2bn.

Currently the ICO market is mostly unregulated but Switzerland, Singapore and Hong Kong have issued some rules. It is unlikely that the market will stay unregulated, however, and this may legitimise cryptocurrencies. ICOs could then become an alternative to IPOs. At the moment, organisations raising cash via an ICO may experience difficulty finding an entity to bank with unless they complete KYC/AML checks and the market is therefore setting some standards in the absence of a regulator. ICOs are currently banned in the US, however.

Over 250 crypto funds have been set up in the last 18 months. The crypto exchange landscape is dominated by a number of large players across Asia, the US and the EU, although a number of traditional institutions have announced plans to enter the crypto space. It is therefore on the cusp of moving mainstream.

Likely trends

Gartner are predicting that, by 2022, at least five countries (including one G7) will have issued fiat-backed crypto currency. Trends in this space are likely to be:

- increased regulation
- regulatory enforcement
- more institutional players
- new business models and innovation.

Conditions for blockchain success

Blockchain needs the right conditions to be successful as follows:

- Multiple parties share data – multiple participants need a view of common information
- Multiple parties insert data – multiple participants take actions that need to be recorded
- Requirement for verification – participants need to trust that the actions that are recorded are valid
- Intermediaries add complexity – removal of intermediaries can reduce cost and complexity
- Interactions are time sensitive – reducing delay has business benefit
- Transactions interact – transactions created by different participants depend on each other.

NEDs can ask questions around the above to ascertain whether blockchain is the right answer for elements of their business.

The technology is still maturing and the business potential of blockchain remains at an exploratory stage. It is, however, likely to be a disruptor to business models and so, whilst it is fine to be anywhere on the spectrum between being sceptical or evangelistic about blockchain, ignoring it is not an option.

US$435bn ***market cap of crypto currency market at April 2018***

US$5,961m ***raised by ICOs in first quarter of 2018***

By 2022, ***at least five countries, including one G7, is likely to have issued fiat-backed cryptocurrency***

Cyber security – Stage 1

Cyber threats are very real and are having a huge impact on a wide range of businesses.

However, this is not just a technology issue. It belongs in the Boardroom and is one of risk tolerance. The goal should be to accept the right amount of risk in the context of the company's competitive strategy in a digital age.

Boards need new skills, management, tools and language to lead in the digital age but there are basics – both technical and behavioural – which should also be in place and need to be measured.

PwC/third party experts:

Richard Horne
richard.horne@pwc.com

Dr Stephen Page
Independent NED
sp@spmailbox.net

Need to know

- Cyber threat continues to grow with an ever-expanding array of tools available to potential attackers.
- Boards have a responsibility to a wide range of stakeholders to protect information assets.
- A framework was introduced to suggest key areas NEDs could focus on to ensure cyber risk is being appropriately managed – see further below.

This workshop began with a look at the threat environment. We live in an era of rapid, revolutionary change enabled by technology. There is much greater consumer engagement via online platforms and more complex integrated supply chains with business partners sharing data, often via Cloud models. At the same time, there is rapid global knowledge exchange – sometimes resulting in innovation sharing and access to rich data sets among both external and internal communities. There are also changes to how we work with flexible working further enabled by portable devices. This highly connected world heightens cyber risk.

In many ways this is an exciting time to be a business leader. However, there is a dark side to these exciting times with a dramatic growth in cyber threat over the last few years due to the greater attack surface that increased technology provides. Today there are more potential adversaries with more power, more access, more motivation and more impact. Often there are devices that could provide a route into a company's systems that are not even considered, such as vending machines in offices. Other attacks can come through networks that individuals might connect to, e.g. breaching the Wi-Fi in hotels.

Managing information risk is critical as failures can lead to economic loss, reputational damage and, in some cases, risks to safety. A diagram produced by the National Crime Agency indicating the cyber crime ecosystem illustrated how criminals are increasingly organised and sophisticated, making use of the tools of the digital world both legitimate and otherwise. Nation state tools, once used, are often available to download and, in some cases, even come with a demo and help function.

Current snapshot of cyber threats

The workshop reviewed current threats as seen by our clients, observed through our Forensic capabilities and reported by UK government sources. Topical areas of concern include:

- a wide variety of attack vectors are now common worldwide (e.g. Distributed Denial of Service, password attacks, ransomware, malware, credential stealing, fake software, man-in-the-middle attacks)
- leakage of customer records (hundreds of millions)
- organised criminal groups adopting a more aggressive posture (extortion, ransomware, etc.)
- increasing scale and sophistication of attacks, especially in financial services (exploiting business processes)
- increasingly fragmented landscape gives more opportunity to steal data (sharing of data behind the scenes)
- Internet of Things risks beginning to be realised (webcams, DVRs)
- state-related targeting and penetration (destructive attacks/industrial control systems, supply chains and professional service providers)
- politics, ethics and regulation (including GDPR)
- insider threat (corrupt, well-meaning, unintentional)
- continued rise of technologies which are outside reach of law enforcement.

More than 40% of all log-in attempts are malicious and political tensions are now mirrored in cyber space. Customer behaviours have also changed and, as people have a shorter expected response time, the conversion from being slightly unhappy to very angry happens more quickly. All of this is amplified in the social media space, often by influencers not directly affected. Additionally, criminals will attack customers of a consumer facing business directly at the first sign of a weakness and therefore fraud and cyber teams need to be connected and communicating.

Recent large scale attacks include:

- Equifax which had personal data of 143m individuals taken through unpatched internet-facing vulnerability.
- WannaCry ransomeware which infected more than 230,000 computers in over 150 countries, exploiting a vulnerability in Windows 7.
- A variant of Mirai (a botnet) which attacked modems and routers through a maintenance interface impacting c900,000 Deutsche Telekom routers.

The recent Petya attack was discussed as this was a previously unseen ferocity of malicious code. It appears to have arisen through a compromised update to accounting software utilised throughout Ukraine and used high access administrator privileges to spread without human intervention. Petya rendered all of a company's IT inoperable within a couple of hours including business systems, emails, company phones, etc. One organisation was run using WhatsApp for several days following the attack.

Unlike Wannacry, Petya did not exploit unpatched software but the global architecture of systems. Many companies that have grown via acquisitions have simply 'plugged in' new systems and so NEDs should query how IT has been integrated in acquisitions and whether overseas organisations need access to the entire corporate network or can be 'ringfenced'. NEDs need to understand what the risk appetite is in relation to bolting on acquisitions, having flat IT structures, etc.

There is also an increasingly hostile climate which encourages data theft and the ethical complexities of 'LuxLeaks', the 'Panama Papers' and the Wikileaks publication of Sony internal emails were considered. A number of media outlets and others have developed sophisticated tools which assist leakers to deposit large volumes of stolen data for public inspection. This can be helpful (in the case of whistleblowers) yet also damaging (e.g. where collateral damage occurs as a result of bulk exposure of commercially and personally sensitive data).

Implications for Boards and NEDs

The Board has a significant responsibility – to investors, regulators, insurers, employees, customers and suppliers, amongst others – to protect information assets. This covers everything that might be of value to other parties including:

- intellectual property, inventions
- financial integrity
- supply chain, process integrity
- customer personal data
- supplier commercial data
- market critical data
- pricing, sensitive algorithms
- safety critical systems
- …and anything else where failure would be embarrassing.

The richer the data, the greater the threat plus social media amplifies the risks. The General Data Protection Regulation (GDPR) has been helpful in working out where an organisation's data is but this is just a first step in terms of cyber defence. People can also have very different views of the risk involved. With Millennials the default position is to share. Part of the issue is that information resides in many places and the sheer volume of data is a real problem.

Cyber security is Board business. There is a close link between digital innovation and cyber risk and this needs to feed into the Board's overall risk considerations. It is about risk tolerance.

The Board has a role to play in direction setting to:

- establish the risk appetite
- assess (and continually re-assess) the threat and its implications for strategy
- help management set values, behaviours, beliefs, limits and ethical boundaries
- help to solve 'big' questions of structure, strategy, pace, disclosure, ethics.

The Board needs to be supported in this by the top executive team – not the IT people – who can assess whether a step change is needed and drive pace, energy and culture. Executive management should:

- deliver a mitigation programme to close any gaps – at the right pace
- define policies and operate controls in line with the Board's risk appetite
- appoint senior leaders (not just IT) with accountability and influence
- sustain insight and capacity across IT, commercial and throughout line business
- develop an appropriate culture in line with the Board's risk appetite.

In terms of the Board's assurance role, directors should:

- inspect measurement systems for focus on the right outcomes
- assess strength and independence of assurance
- assess (and seek proof of) crisis readiness.

Boards are often at a stage of 'awareness' of cyber issues and are 'updated at' but need to move at least to a stage of 'understanding' where an appropriate risk appetite has been developed with management information that supports this.

A discussion then ensued around what NEDs could do in practice to manage cyber risk. It was suggested that there were six areas in particular where NEDs need to be confident that an enterprise is on top of this:

Priorities

- ensure that the right priorities have been set to protect what matters and in light of the threat intelligence
- look at the strategy, organisation, governance and enterprise security architecture
- ensure that strategic decisions consider digital risk appropriately.

Seize the advantage

- set risk appetite
- check that digital trust is embedded in the strategy
- ensure compliance with privacy and regulation
- challenge the balance being struck between speed to market and ensuring confidence in the security of new products and services.

Their risk is your risk

- understand the extent of an organisation's interconnectedness.

People matter

- build and maintain a secure culture so that people behave appropriately in the 'moments that matter'
- identify key individuals in sensitive/critical roles who could have disproportionate impact on the organisation if they acted maliciously.

Fix the basics

- ensure that an organisation's IT systems are well built and operated.

It's not if but when

- ensure that an intelligence-led, rapid cyber response plan is in place as part of its crisis management strategy.

Undoubtedly, in many cases, the Board needs to be spending more time on this area. There should be someone with digital age knowledge in the Boardroom and data needs to become a currency around the Board table. This has become increasingly important now that GDPR is in force and individuals only have to cite distress, rather than proving financial loss, to claim compensation in cases of data loss/ leakage. GDPR provides a good opportunity to invoke a culture change.

CISO (or CIRO in the public sector) roles are becoming increasingly common and attempts are being made to address skills shortages in this area via cyber security centres of excellence. This is not just about technical skills but also the ability to influence when necessary. Due to its fundamental and all-pervasive nature however, the CEO needs to own the cyber security agenda, supported by the CISO.

The second half of the workshop explored a recent cyber attack which has damaged the operational and strategic performance of a major business. Those present discussed, admittedly with the value of hindsight, what questions the NEDs could have asked to fully understand their exposure and risk.

The conversation covered:

- how difficult it can be to foresee some of the risks involved in large technology investments which are often seen by the Board primarily in terms of business opportunity
- Boards sometimes lack the language and skills to dig deeper
- in this particular company, NEDs, and especially members of the Audit Committee, were under the spotlight for the way in which they may have failed to foresee and mitigate digital risks.

The discussion also addressed a second company which unwittingly provided the pathway through which the attack was conducted and discussed what NEDs on this Board should have done to establish a stronger, safer digital environment. It is vital for Boards today to consider any exposure via their extended enterprise of partners, suppliers, contractors, etc.

The NEDs in this situation could have asked questions such as:

- What is the critical data we want to protect?
- Have we done an audit of who has third party access to our systems?
- What are their defences like?
- Where are the firewalls?
- What level of authority allows third party access and where does this reside?

Conclusion

The workshop concluded with some questions it was agreed Boards might want to consider around cyber defence split into the following areas:

- Do we have the right skills?
- Do we have the right fact base?
- Are we making active, well-founded choices from the top?
- Do we measure and improve?

In terms of breach response, Boards should consider:

- Is there a practised plan for breach response that operates at 'social media' speed?
- Is the organisation ready to manage the market impact of a failure?
- Is the organisation willing to share intelligence with others?
- Are near misses analysed and lessons learned?

Beyond the basics, Boards should discuss questions such as the following:

- What can we actually control? How do we prioritise/ segment?
- How much variation/innovation/flexibility do our people need and what does this do to our risk profile?
- Should we proceed at a slower pace to keep risk under control, especially re digital innovation in an 'agile' business methodology?
- How can we control the risks our suppliers expose us to?
- Can we afford to keep up with our customers and manage risk?
- What personal data should we retain? – ethics vs business value?
- Do we trust our staff? How do we balance control/ monitoring with personal privacy/freedom when lines are blurred between home and work?

Companies are increasingly being encouraged by regulators and others to share information regarding cyber security breaches for the protection of others. Each company will need to steer its own course taking well-reasoned risk choices and executing them well.

68% ***of large UK businesses have identified at least one cyber security breach over the last 12 months***

51% ***of businesses holding electronic personal data on customers are likely to suffer a breach***

£3.2m ***fines for UK data privacy issues in 2016, double the prior year***

Cyber security – Stage 2

No business is immune to cyber threats and the issue of cyber security is firmly on the Board agenda.

For those NEDs who had covered the basics on the cyber security stage 1 workshop and begun to work through cyber issues with their Boards, this session was an opportunity to explore in more detail some of the key challenges at Board level via four important areas:

- ***developing a business perspective***
- ***assessing current state***
- ***improvement recipes***
- ***handling incidents and crisis.***

PwC/third party experts:

Richard Horne
richard.horne@pwc.com

Dr Stephen Page
Independent NED
sp@spmailbox.net

Need to know

- Boards have an important role in 'setting the tone' in relation to cyber security following a thoughtful holistic view of what is important to their business.
- A framework of seven cyber security governance principles developed by PwC suggests focusing on:
  - a real understanding of the exposure
  - appropriate capability and resource
  - a holistic framework and approach
  - a considered approach to the legal and regulatory environment
  - active community contribution
  - incident preparedness and track record
  - independent review and testing.

Context

This workshop began with a recap of the interconnected world in which we live and the consequential heightened risk of cyber attack. A look at the National Crime Agency's cyber crime ecosystem showed, rather alarmingly, the extent to which criminals have organised themselves into a sophisticated marketplace – a comprehensive ecosystem with ready access to assets, tools and techniques for cyber attack. There was also a recap of the latest common cyber security issues and the pain spiral when things do go wrong, as well as the Board's role in setting direction and assuring outcomes – refer to the cyber security stage 1 workshop on pages 29 to 32.

Boards need to take a thoughtful, holistic view of what's important to their business. This is a hard debate to have, often due to a lack of skills and time, and the preponderance of technological terminology. It will also vary from one industry sector to the next. However, the Board has two fundamental roles around executive management's risk control processes and mitigation plans:

- Determining risk appetite – setting the boundaries to frame executive management's work to close the gaps
- An assurance role – looking at the measurement systems and assessing the strength and independence of assurance as well as proof of crisis readiness.

The important role of Boards in 'setting the tone' was discussed, including some of the choices where they need to guide management such as:

- speed to market versus risk control
- data analytics versus ethics and disclosure
- sharing of information versus segmenting the business
- everything in house versus alliances
- trusting employees versus surveillance.

Framework of seven cyber security governance principles

A framework for structuring a Board agenda and having a meaningful cyber security conversation with the CEO was discussed.

At the heart of this framework sits:

Real understanding of exposure

This is a consistent and constantly changing issue which sits at the heart of cyber security. It needs to be a Board conversation about both threat and vulnerability, including issues such as:

- what data is held
- how likely is it to be of interest to others
- how many places the organisation's systems connect with the outside world
- what types of attack are common?

Around this core issue are:

- appropriate capability and resource (going beyond the IT department and also at Board level)
- holistic framework and approach (wider than technical and includes culture plus a real understanding of business processes)
- considered approach to legal and regulatory environment (which is complex and needs to be understood)
- active community contribution (sharing details of attacks with others externally)
- incident preparedness and track record (important for investors as responding well can be brand-enhancing)
- independent review and testing (including outside opinions and the use of ethical hackers).

The workshop then moved into detailed debate around four key areas where NEDs can focus to get under the skin of cyber security risk. In each area, in addition to discussing the issues, useful frameworks were provided as well as case studies of approaches that have been seen to work.

Developing a business perspective

Boards need to consider this in three areas:

- what kind of organisation is the company
- what data does it hold
- what types of attack might it need to defend against.

It is vital for the Board to first assess what the company is and does and then to determine how cyber affects the sector. Characteristics to consider in determining which aspects of the business yield high cyber security risk include:

- Economic sector – risks vary between sectors with some intrinsically higher risk than others
- Geography – defence mechanisms may not be fit for purpose everywhere
- Business change – often not appropriately taken account of in management information
- Business operations – e.g. industrial/supply chain
- Ethics and culture – e.g. how much customer data is held, particularly pertinent with today's desire for a 'single customer view'
- Risk appetite – derived after taking account of all of the above.

Consideration of these special characteristics help Boards to make choices and set a vision/strategy for cyber risk.

Bearing in mind that it would be prohibitively expensive to protect everything fully, Boards also need to consider what matters most which is not always an easy exercise but is invaluable in the long run. A collective view is needed as different functions will value different data.

Boards need to ask what types of data they hold, such as:

- personally identifiable information
- financial information
- supply chain information
- pricing/commercial information
- mergers and acquisition information
- Board papers/strategic intentions

and what is the purpose of protecting it:

- regulatory
- stakeholder interest
- sensitivity
- evidence
- reputation
- share price
- trust
- availability.

There was some concern among the NEDs that it might be difficult to defend a position of not protecting everything but Boards often need to make such choices. The 'crown jewels' need to be identified along with where they are and who can access them.

Boards should also reflect on the types of attacks from which they need to protect the business. A framework was presented to help with this consideration by mapping attacks from low, through to medium, then high and finally advanced levels of sophistication and split between external and internal threats. For external threats, from low to advanced sophistication, these ranged from:

- opportunistic or non-targeted attack
- targeted, remote attack
- targeted attack with internal assistance
- unconstrained attack.

For internal threats, the spectrum was:

- unknowing insider (human error)
- malicious insider acting within authorisation
- malicious insider acting outside authorisation
- advanced and expert insider.

In relation to the four types of external and internal attacks listed above, banks should be able to defend against at least the first three levels of both lists. The fourth level is very advanced but could be relevant for defence organisations or national/global infrastructure.

Rogue employees can be difficult to identify so systems need to be constructed so that any one individual cannot do too much damage. It was noted that the Centre for the Protection of National Infrastructure (CPNI) has issued a paper addressing managing the employee threat.

Questions that the Board (or a subsidiary committee) can ask in this area include:

- What data do we capture, create or handle and what are our obligations to protect it?
- What is our appetite for risk and against what type of adversaries?
- What may impact reputational risk?
- How do we apply priorities? What have we decided not to protect?
- How do we set the tone? What questions should we address?
- By when should risks be reduced? What sense of urgency is required?

Developing a business perspective in the ways suggested above can lead to a more meaningful risk appetite.

Assessing current state

The workshop moved on to discuss how Boards can get beyond narrow presentations from IT and delve into the real state of cyber readiness as a business issue. Cyber security can be a root cause for many other types of risk, such as fraud, reputation, business continuity, etc. The scope of cyber activities pervades all areas and therefore Boards need to probe across:

- Strategy, governance and risk – are there people with the right skills, experience and capabilities, that are 'future proofed'?
- People and culture – is there training and awareness with focus on key roles from a risk perspective?
- Threat, intelligence and capabilities – including how risks are changing as new technologies are adopted.
- Information discovery and management – what is critical and how well protected is it?
- Connections – which partners does the business share with and are they properly protecting the information?
- Testing and crisis management – how well would the company respond to an incident?
- Business processes – are these appropriate and resilient?

Answering each of the above questions may require significant work led by the CEO/CFO. NEDs need to ensure there are measurement systems in place to ensure the executives are dealing with this appropriately and a Board sub-committee may need to be set up to monitor this at least initially. Connections with third parties need to be considered as today's extended enterprise increases risk.

There was a discussion around penetration testing and the fact that this has changed. Traditional penetration testing assesses vulnerabilities and poor configuration within IT systems. However, as the tools, tactics and procedures of attackers have become more sophisticated, their attacks now tend to focus on the end user. A new approach to penetration testing is therefore needed that is intelligence led, value driven and has a strategic focus. NEDs should not take false comfort from penetration testing which is too narrow or too technical. Simulating the most likely attack and seeing how the responses cope can be good practice. Sharing of threats is also valuable and likely to become more developed going forward.

NEDs should seek strong metrics which demonstrate the strength of cyber resilience, not just the volume of attack attempts. Examples include:

- % of systems accredited to security standards
- % of desktops at target patch level
- % of encrypted laptops
- number of unrecognised assets on local area network
- number of supplier contracts with clauses for information protection
- number of staff with critical access with up-to-date vetting
- number of days between employee role change and systems privilege change
- average time from incident detection to escalation/resolution.

Boards can ask to see where the exceptions are and how they are getting fixed. NEDs recognised that asking for some of these measurements will expose helpful gaps in how well risk is controlled.

Questions the Board may wish to consider when assessing the current state include:

- Do we have adequate breadth (e.g. people, technology, engineering, business process, commercial, legal)?
- How can we confirm that our policies reflect our risk appetite?
- How can we confirm whether our policies are being implemented thoroughly?
- Have we covered the basics sufficiently to preserve our reputation?
- To what extent does a lack of incidents indicate that we are secure?

Getting 'the basics' right can reduce the level of 'noise' so that it is easier to focus on the more complex areas. However, it needs to be a dynamic process as businesses and therefore risks change. Many of the challenges around cyber security are not IT related but how the organisation is configured.

Improvement recipes

Risk mitigation covers a broad scope of activities in terms of the business environment, the security environment and control frameworks. The PwC cyber capability framework was discussed to indicate how companies can identify, protect, detect and respond. If legacy systems make good protection too time-consuming/costly, there may be a need to over-invest in detection. However, this is not just about buying tools but about building a capability that can then invest in the most appropriate tools.

Control frameworks need to be in place to ensure the basics are covered. NIST is becoming a global standard and the UK Government has also produced Cyber Essentials and Cyber Essentials Plus (the accredited version).

A few of the most common risk-reduction activities were considered – asset control, legal policy, employee access, digital user authentication, cyber incident detection and industrial control systems – the message being that this should not all end up with the CIO but ownership should be spread right across the organisation and the CEO needs to take the lead on this.

Questions the Board can ask in this area include:

- Are we seeing the sorts of actions we should expect from management?
- How do we know whether these are sufficiently complete?
- Are the actions progressing fast enough?
- How do we know where we are on the journey?

Handling incidents and crisis

The final section of the session began with a look at a case study showing a typical financial services breach response. The incident involved 500 compromised machines, 35Tb of log data, 1,300 formats and 600 billion events requiring analysis. The attack was ten months work which ultimately yielded $8m for the fraudsters. As a result, to get the full picture of what had happened took considerable time. The information a company initially has on discovering a breach will be very limited and there is therefore a need to take care with any messages that are communicated to avoid early false conclusions. On the positive side, the level of anomalous activity provides plenty of 'trip wires' for detection.

A second incident illustrated that a breach may not always be technology related as it centred around passwords. Some 'intelligent guessing' based on a previous LinkedIn breach, permitted the attackers to gain entry after a few attempts. Once in the system, they found individuals emailing passwords to themselves when they were renewed. Eventually, the administrator's password was located and a more extensive attack became possible. This second case study illustrates the criticality of access controls which are often a point of weakness in organisations.

There was a brief consideration of the different types of crises – classic, rapid onset events, hidden crises, operational disruption, strategic disruption. Major classic crises (e.g. fire, flood) are generally easy to detect but with IT it may not be obvious that a crisis is developing until a significant impact is experienced, although often there are warning signs along the way.

NEDs should agree in what circumstances management need to bring the Board in to help shape the response to a crisis. They should also bear in mind that incident handling requires capabilities to both detect and respond. This is an area that lends itself to scenario planning. Playbooks should be developed for a cyber security breach, taking into account that at the point at which the company becomes aware of a breach, there are likely to be many unknowns in terms of what has happened and what has been impacted. At the same time, customers, regulators and MPs may all be demanding explanations.

Questions the Board can usefully ask are:

- How are investments prioritised between prevention, preparation, response and recovery?
- Has the Board recently practiced its response to a cyber crisis, including with deputies?
- Who has authority (training, decision-making remit) to respond in less than an hour?
- How robustly are minor incidents handled? Are we signalling the Board's risk appetite and values to employees and suppliers?
- If we discover a long-term penetration, can we determine what data has been accessed, changed or exfiltrated?
- Is the action plan for emergency management thorough, well-rehearsed and effective (including with no IT)?
- At what point would a decision be made to 'shut the shop' and who has that authority?

It was noted that regulations in Europe have changed such that the regulator now needs to be notified of any breach.

Conclusion

While NEDs can make great use of existing skills, such as probing gaps in controls and seeking evidence of management's measurement system, for many businesses it may be time to address any shortfall in digital skills around the Board table. Most Boards need at least one NED who is fluent in digital issues which should span both innovation and cyber risk, and both new and old technologies, in order to lead a business in the digital age. Some Boards would also benefit from a specialist Board committee (e.g. information risk or digital) but this cannot substitute for an adequate understanding and overview by Board members.

In order to move from an awareness of cyber security to an understanding, NEDs should seek to ensure that there is:

- a risk appetite based on a Board grip of what data is held, why, for how long and accessed by whom
- enterprise MI which shows actual risk profile and compliance
- Internal Audit meaningfully assessing the above
- a fact base about how cyber risk is shared with suppliers and business partners
- agreed policies compliant with data protection law
- a practised crisis plan, including with deputies, and MI which shows time from event to detect to act
- a CEO and Chairman who are confident to address shareholder questions.

The concluding questions at the end of the cyber security stage 1 workshop were revisited as a good starting point for NEDs – refer to page 32.

Finally, workshop participants were provided with three supplementary papers which are available to NEDs on request as follows:

- a more detailed breakdown of the seven cyber security governance principles authored by Richard Horne
- a paper describing how Board conversations need to change for the digital age and setting out a role description for a 'digital/technology NED' authored by Stephen Page
- a booklet from the CPNI describing how individuals can get better control of their digital footprint and reduce their exposure to cyber attacks led by social engineering.

***223** days = typical time between cyber breach and impact*

***£1.9bn** committed by Government to protect UK from cyber attacks*

*Only **26%** of breaches currently lead to information being shared externally other than to a cyber security provider*

Social media, digital tools and online hygiene for NEDs

Social connectivity, the merging of home and work, instant access to powerful apps and tools via mobile phones have all changed how people live and work. Increasingly individuals participate in rich social networks and use a bewildering array of tools throughout their digital lives.

The workshop was an opportunity to gain an understanding of some common digital platforms and tools and also consider online hygiene, with a specific focus on how NEDs can use these tools in their professional and personal lives.

PwC/third party experts:

Nick Masters
nick.masters@pwc.com

Sacha Wooldridge
sacha.n.wooldridge@pwc.com

Dr Stephen Page
Independent NED
sp@spmailbox.net

Need to know

- The growth of social media has resulted in a blurring of personal and professional lives.
- Employees, customers and other stakeholders will be making use of an array of social networking, image/video based and broadcasting/streaming platforms.
- These platforms, and their equivalents overseas, have millions, and in some cases, billions of users so their power and influence should not be underestimated.
- There are also numerous digital communication/collaboration tools that many are employing.
- In their personal capacity as technology users, NEDs should focus on the following areas, setting their own risk appetite and making a well-informed set of choices, to ensure they do not become 'the weakest link':
  - social engineering and phishing
  - social media
  - passwords
  - handling data
  - internet browsing
  - working remotely
  - physical security
  - encryption.

Context

Social media is a dominant force shaping society. Everybody has a digital footprint whether they want one or not. A photo indicated how events are captured by people present as they happen and shared, now that the use of smart phones has become all pervasive. Facebook with two billion active users is now bigger than the entire internet in 2008.

However, there are risks to the huge explosion in social media as PwC has experienced directly. The story of 'Heelgate' where a PwC receptionist employed by a contractor was sent home for not wearing high heels was shared 10,000 times in 24 hours. After 36 hours the story had been seen by 30m people. Similarly, the envelope mix-up at the Oscars dominated the news for over a week.

This social media engagement is now of a level not previously contemplated. However, it is worth noting that people choose what they want to see. Companies or individuals therefore need to be invited into the user's world by finding ways of making things interesting and relevant to people. Social media is about building trust through listening and engaging and not just about broadcasting.

Common social media platforms

The best known **social networking platforms** in the UK are Twitter, LinkedIn and Facebook.

- Twitter is now widely used by business for engagement with journalists, regulators and politicians, as well as by individuals. It has a direct messaging service which can make it surprisingly easy to get to influential individuals. Often people will have separate personal and business Twitter accounts. When an incident occurs, the immediate reporting on Twitter is much faster than verified news channels. Equally, good customer care can be facilitated by Twitter.
- LinkedIn is a business networking site and is extensively used by recruitment consultants. There are two schools of thought re accepting contact requests from accepting everyone (useful if pushing out content) to only accepting invitations from people genuinely known and relevant.
- Facebook started as a platform for sharing with family and friends but is now also used by businesses, particularly in the US and by retail and consumer businesses, and this adoption is becoming more widespread.

Common **image/video based platforms** are Instagram and Snapchat which have almost no text.

- Instagram is used extensively by individuals. Photos and very short videos (up to 20 seconds) are posted on personal profiles but it is often quite staged and more about broadcasting than engaging. Very short bits of text can be added and there is the ability to link to other profiles.
- Snapchat is an app for connecting with friends or following famous people. Photos and up to 10 second videos can be posted but disappear once viewed. Following an update in the summer, Snapchat can also identify where your friends are as the default setting is that location is made available.

It is also worth bearing in mind with all these 'temporary' image platforms that somebody could still take a screen grab prior to deletion, although Snapchat will notify the photo originator if someone has done this.

PwC is using these platforms as follows:

- Instagram – to share events such as Ride the Nation and One Firm One Day and show a more personal side to the firm
- Snapchat – used on campus with a geofilter for recruiting and to distinguish the firm from its competitors.

Common **broadcasting/streaming platforms** are You Tube, Periscope and Facebook Live. You Tube is now the second biggest search engine after Google reflecting a significant shift in behaviour with users preferring videos to text, particularly among the young.

There is a lot of common ownership of these various social media platforms:

- Instagram is owned by Facebook
- You Tube is owned by Google
- Periscope is owned by Twitter.

These owners are therefore extremely powerful in the influence they can exert, enabled and underpinned by their vast repositories of personal data. This is enriched by augmenting social profiles with search history, browsing history, purchasing patterns and email traffic on 'free' services (e.g. gmail).

This information power allows platforms to provide 'relevant' advertising but also to shape the content that users see.

There are also some very significant international platforms including:

- VKontakte – Russian language platform, a cross between Facebook and Twitter, with over 400m users
- WeChat – Chinese language platform with around 1bn users, both social and commercial, to message, share and buy
- Tencent – Chinese language Twitter-style app with 800m users
- Weibo – Chinese language Facebook clone with 250m users.

The majority of social media platform use is on smart phones or tablets.

There has been more interest in Facebook by the business community since newsfeeds were introduced. As a result, Facebook for work has been set up as an information sharing tool and is sometimes used as an internal social media network by some smaller organisations.

An official Twitter account will have a blue tick in a circle to differentiate it from any bogus accounts. With Facebook and LinkedIn, official company pages will also have been verified.

LinkedIn is a safe place to start a social media journey and business people should ensure that they have an appropriate and carefully crafted profile. PwC is now often asked for LinkedIn profiles in pitches, rather than CVs, as there is the view that people are more accountable for profiles that are publicly available. LinkedIn can effectively become a 'black book' of contacts, even if someone moves organisation, and there have been some complex legal challenges when individuals have taken their 'personal' LinkedIn contact lists to another employer.

Posting something also has more of an impact on LinkedIn as people do not post extensively on this platform so content tends to stay for longer versus Twitter which updates every few seconds. Only 2% of LinkedIn subscribers are very active users. A number of groups have formed which share useful content, e.g. Boards and Advisors.

With all social media platforms, however, it is worth bearing in mind that linking with like-minded individuals/groups can cause individuals to operate within a bubble and reinforce beliefs and so a spectrum of views should be sought.

Social media is changing how trust in people, products, etc. is built. Most millennials will seek social consensus rather than expert views, e.g. rating Trip Advisor above a Michelin Guide and a 'much liked' article over the choices of a newspaper editor.

Individuals use social media for:

- news – sharing articles with followers to demonstrate individual is up to date
- marketing – including pre-approved materials
- personal – more likely to engage if a message comes from someone you trust
- specialism – demonstrating expertise

because it is:

- free
- easy to access
- an instant communication tool
- a gateway to a huge network
- a direct link to journalists/stakeholders/senior individuals

all of which help with influencing or getting a message out.

Individuals should Google themselves to see what online profile they have. Most are often surprised to find they already have a substantial digital footprint.

Social media communications are often timed for the morning and evening commutes when people tend to be on their phones and between 10 and 11pm when individuals check their phones before bed.

Language is an important part of social media communications and needs to be appropriate to the platform – generally more casual and less formal. Emojis are used extensively, particularly in Twitter where there are only 280 characters (approx. 30 words) and emojis can help with tone. There are also many abbreviations in text speak but these are generally best avoided. Hash tags are used in text with key words so that content will be visible to those searching by those words. The more hash tags used, the wider the reach.

Within PwC, a scheme with millennials 'reverse mentoring' partners has built confidence in how to use social media. One partner who tweeted 30 times in a month (less than 400 words in total) reached 23,000 people which shows the reach possible.

However, with this reach comes risk. Often you may be a first mover which can have inherent risk and sometimes you can feel as if you are waving in a field if content is not picked up. Trolling is always a risk, even with innocuous posts, and it is best not to engage with it. It is also always worth applying 'The Daily Mail' test to consider how a post might appear to the man in the street.

Digital communication and collaboration tools

Another fundamental digital-age change is a shift from big firm supported IT systems to a personal 'toolbox'. These tools are often simpler and faster so that even complex business processes can be done quickly, cheaply and efficiently. There was a brief look at some of the most common online communication and collaboration tools as follows:

- Meetings – Webex, Google hangout, Skype
- Messaging – WhatsApp, Telegram, Yo
- Projects – Slack, Trello
- Crowd-sourcing – Doodle, Survey Monkey
- Sharing – OneDrive, Google Drive, Dropbox.

Slack has the advantage of capturing discussions in streams by project so is commonly used by start-ups, particularly during project development. Trello is more of a traditional project management tool for use on mobile devices.

Doodle is a quick scheduling tool for getting people together and comparing calendars while Survey Monkey enables fast sharing of views through simple online polls and surveys.

Sharing platforms, where information is accessible to those given access, enable a group of colleagues to work on the live version of a document. Dropbox is frequently used by the media where large file sizes are common.

NEDs should have an awareness of these digital tools, as they may be useful for them as individuals but also employees within their organisations may use them.

Questions to consider

The social media section concluded with a number of questions individuals may wish to consider:

- What do you what you want to be known for; what are the best channels for this?
- Do your profiles and shared content reflect this?
- Are you listening and learning from what's going on?
- Have you researched the groups and conversations to join?
- How do you find and connect to influencers on your topics of interest?
- How can you build your influence? Answer questions and share compelling content to engage your audiences.
- Is it appropriate? Always review what you propose to say and think about the language you use.
- Do you have a 'digital toolkit' of quick ways to get things done individually or in a group?

Online hygiene

The importance of online hygiene was illustrated by a case study exploring the number of organisations that track an individual through their digital footprint from the moment they wake until they complete their journey to work. Even more eye-opening was a list of more than 50 trackers, cookies and connections logged by Lightbeam and Ghostery in a freshly-installed browser after opening just the home page and one article in The Guardian.

Although GDPR in theory gives individuals more control over their data, one particular site presented the user with 300 tick boxes and multiple options is not uncommon.

Effectively, we are all paying for the use of search engines and 'free' email by revealing a little more personal information each time. It is therefore important that individuals are aware of their digital footprint and choose personal behaviours to match their risk exposure.

This was explored further by focusing on eight key areas:

Social engineering and phishing

Psychological manipulation can encourage people to perform actions or divulge confidential information without being conditions of the right to share personal data. Individuals should therefore:

- be suspicious of unsolicited calls or emails from individuals asking about employees or information, even if the caller seems to know a lot about you already
- not reveal personal/financial information by email or respond to email requests for this information and not authorise transactions by email alone
- check emails for odd phrases and word choice based on your knowledge of the sender
- pay attention before you click on anything, even if it claims to be from someone you know.

Social media

Social media is useful for staying in touch with friends, family and work colleagues. However, personal information shared on social media can also help attackers commit identity theft and fraud as they connect data from various sources.

The terms and conditions of some social media platforms will give them the right to share personal data or reuse individuals' content in unhelpful ways. Individuals should also be aware that their own friends/contacts may have uploaded their entire address book to LinkedIn thus indirectly providing their information. After a LinkedIn account has been created, it is possible to go into settings and change privacy details but this is often not an opaque process as privacy policies and options are often deliberately complex.

Individuals should therefore:

- review the privacy policy and terms of service before signing up for an account
- set privacy options carefully and revisit them periodically to check for newly-invented settings
- never provide a work-associated email to social media
- not post age, date of birth, address or phone number
- decide what online footprint is appropriate and ensure your friends understand this too, e.g. tagging in images, uploading your personal details from their address book
- be wary of connection requests from strangers or fake friends
- remember anything online might be seen by people not in the intended audience and passed on to others
- think about the consequences of sharing your location.

Passwords

Poor password habits are widespread, allowing attackers to compromise email accounts, business applications, social media profiles and bank accounts. There is a need to find a balance between making passwords hard enough for computers to have difficulty finding them but not too difficult for people to remember.

Strong passwords can include:

- length – longer = stronger
- complex or not?
- base passwords on a phrase not a word
- do not re-use passwords on multiple sites
- consider using a password wallet.

There is conflicting guidance on changing passwords regularly due to the behaviours that result. Frequent changing of passwords sometimes causes individuals to email passwords to themselves leading to exposure from hacking but password wallets can also be hacked. Criminals seeking access to data will exploit the weakest link which may not be the password itself but the password reset mechanism and therefore understanding how lost passwords are reset is also important. Risk aware individuals can mitigate this by giving false answers to set questions when setting up accounts. Using a password wallet is now deemed better practice than regularly changing passwords.

Two-factor authentication ('something you have and something you know' – e.g. a password plus a code that is sent by SMS or generated on your personal mobile and valid for a short period only) is powerful and should be used wherever available. NEDs are encouraged to try two-factor authentication on their Amazon and Google accounts, for example.

Face recognition and touch ID are also improving this area.

Handling data

Modern technologies such as the Cloud make it easy to store and share data. However, these benefits come with significant risks, including reduced data confidentiality and trusting someone else's security.

Individuals should:

- only gain access to the data you really need and delete it when finished
- use business-approved storage for handling work data
- ensure email recipients are correct (email address auto-complete can create problems)
- avoid sending sensitive, unencrypted data outside your organisation via email or by using public Cloud sites (e.g. Dropbox or Google)
- understand what data you hold and where it is stored (e.g. password protected .zip files, on your desktop).

Knowing what data you have and storing it safely in approved ways is a good place to start. Even better is not to hold the data in the first place – leave it in the office whenever possible. Diligent is a popular Board paper sharing app used by many companies.

Internet browsing

Websites that appear to be legitimate could contain malicious or harmful links/attachments or be falsified in order to fraudulently collect personal and commercial information.

Individuals should:

- keep their browser and operating system up to date. If practicable, disable Silverlight and Java
- pay attention to website URLs, reading right to left. Malicious websites often look similar to a legitimate site (e.g. an 'm' instead of 'n') or use subdomains (e.g. barclays.foo.com rather than barclays.com). If in doubt go manually to the company website rather than clicking on a link
- be suspicious of links to secure content that do not include https (padlock, in some browsers) or appear (pop-up) unexpectedly while using the Internet
- not download apps that appear suspicious or have not been developed by a recognised body or organisation
- only use business-approved software to format, translate or send documents both internally and externally.

It is likely that domain names such as .pwc or .barclays (i.e. without the .com) will soon become prevalent.

Working remotely

Working remotely often requires employees to access confidential, commercial and sensitive information, offering additional opportunities to malicious actors.

Individuals should:

- deter shoulder surfing by viewing commercially sensitive data or documents in a secure location
- connect only to Wi-Fi connections that are trusted and password protected. Only use 'https'(SSL-secured) websites and mail when using Wi-Fi in hotels, trains etc.
- use work email accounts only to view sensitive information or data
- not bring work devices or documents to locations (e.g. restaurants) where they could be stolen.

Physical security

Physical security of devices is important but often overlooked. Poor security puts data and devices at risk of being stolen and can result in identity theft, business disruption or bodily harm.

Individuals should:

- lock devices such as laptops, PCs, and mobile devices automatically when they are unattended. Use a strong (i.e. long) password or PIN to lock them.
- know how to lock your device instantly (button, mouse to corner of screen etc.) and get into the habit
- know how to wipe your phone/iPad remotely (e.g. set up Find my iPhone; keep a record of the IMEI number)
- immediately notify your security or IT department if your device has been lost or stolen
- discourage tailgating. You are the most effective security measure, and are empowered to challenge unfamiliar faces.

The majority of data has a back-up in the Cloud so can be restored if you need to wipe your phone.

Encryption

As global commerce expands online, strong encryption is becoming essential. Weak or poorly-implemented encryption leaves personal and corporate data exposed to attackers. Individuals should:

- note that strong encryption adds another layer of protection in addition to vigilance and physical security
- activate encryption on work and personal devices and use only apps which support secure storage
- when possible, encrypt data in transit and at rest
- use strong passwords to ensure secure encrypted devices (e.g. complex PIN codes for mobile phone)
- remember to encrypt back-ups too.

Setting risk appetite

There was much discussion of the need for every NED to make a well-informed set of choices based on the risks and the data they may hold now and in their future career. This risk appetite will shape the nature of their digital footprint and the level of protection that is necessary. Individuals need to decide personally where they are on the spectrum from 'totally open and trusting' to 'private and paranoid' and then set their risk appetite accordingly.

We discussed several profiles on this spectrum from a digital native who automatically and freely shares sensitive data to a highly risk-averse NED who operates several online personas choosing what to share and implementing strong protections for sensitive information. It is possible that this risk appetite may be different for different areas, e.g. more risk averse with bank account data than other less sensitive information. Making the right decisions about social participation and information protection is becoming one of the critical choices for NEDs. NEDs need to take a lead on security to set the tone.

2 bn *users on Facebook*

280 *characters to a tweet*

Charities – how to adapt and thrive in the current climate

Whether it is the impact of the EU referendum vote or widespread economic, political and social change, these are times of great flux for charities. There is both an opportunity and a necessity for charities to rethink how they approach strategy, leadership and governance, as well as the resources they draw on and the relationships they build, to deliver greater impact in an increasingly complex world.

The workshop provided the opportunity to discuss a number of issues relating to the charity sector including clarity of purpose, impact, reputation, effective use of resources and collaborations/mergers.

PwC experts:

Ian Oakley-Smith
ian.oakley-smith@pwc.com

Jill Halford
jill.halford@pwc.com

Daniel Chan
daniel.y.chan@pwc.com

Need to know

- The charity sector has been through a difficult time over the last couple of years.
- Scrutiny of the sector by a large number of stakeholders has intensified.
- Charities are becoming more focused on their purpose and reporting on their impact.
- Strong governance needs to be in place and trustees need to reflect on the effective use of resources.
- In some instances, collaborating with others addressing a similar need, including possible mergers, may be appropriate.
- There is a need for strong decision making and experienced NEDs will be well placed to take a lead in ensuring that their charity Board is effective.

Context

The workshop began with a look at the current state of the charity sector. Recent times have been very challenging due to both the economic environment and, more recently, the reputational impact of certain examples of inappropriate behaviour in the charity sector highlighted by the media. New Philanthropy Capital, a charity focused on promoting good practice around impact and effectiveness, recently conducted a survey on the state of the sector involving more than 400 participants from all areas. A short video was shown to illustrate three of the major themes that came out as follows:

- a lack of focus
- use of technology
- strength of resources.

These themes have been borne out over the 12 months since the launch of the survey. Charity Boards often don't have the same commercial focus as company Boards. Charities are at different stages in terms of their focus on impact, and using this to inform strategy and, potentially, hard choices.

Although 70% of charity leaders felt they were making the best use of technology, this may not be the case given the speed with which technology is developing.

There is also a need to work collaboratively, think creatively and look again at resources.

Heightened scrutiny

Issues that have been widely reported relating to The President's Club, Oxfam and Save the Children, amongst others, as well as questionable fundraising practices, have resulted in the charity sector coming under intense scrutiny from a number of different stakeholders, including:

- beneficiaries
- staff and volunteers
- funders and partners
- members
- other charities
- the Charity Commission
- HM Revenue and Customs
- Companies House
- the Fundraising Regulator
- the Information Commissioner's Office
- the media and the general public.

The last two years have seen significant damage to levels of trust as the public tend to hold charities to a higher threshold of account. This does not just impact fundraising but also how a charity engages with its beneficiaries, campaigning and many other areas. The duty of both auditors and trustees to report serious incidents has also increased.

Trustees therefore need to think carefully about the risks on the charity's risk register and whether these are complete and relevant. Risk/reward decisions are key and trustees might also want to reflect on the questions they should know the answers to – such as 'how do we ensure compliance with safeguarding risks?' or 'how do we protect vulnerable people from heavy-handed fundraising techniques?'. Trustees should ensure they are getting full sight of what is happening on the ground. They also need to understand the views of their supporters in terms of how they should respond to incidents. Engagement with stakeholders is therefore key.

A Code of Fundraising Practice has been issued by the Fundraising Regulator and there are new disclosures required this year around fundraising activities in trustees' annual reports. Charities also need to consider the guidance issued by the Information Commissioner's Office and, where relevant, the Care Quality Commission.

A Charity Governance Code was introduced last summer and trustees should be aware of this. It is on an 'apply or explain' basis, and therefore voluntary, but represents best practice in terms of governance. At its foundation are the trustee role and the charity context but it also addresses the following seven areas:

- organisational purpose
- leadership
- integrity
- decision-making, risk and control
- Board effectiveness
- diversity
- openness and accountability.

A broader debate around good governance included the following observations:

- diversity of thought is important
- appropriate succession planning and skills gap identification is necessary
- the governance code may help with 'churn', as time limits do not always exist in a charity's governing documents
- a good Chair is vital and can make strong governance happen seamlessly
- an appraisal process should be undertaken with rigour
- trustees with the Chair of Audit Committee role can usefully highlight aspects of the governance code that are not being met
- above all, charities need to be clear as to their purpose and make decisions with a focus on the beneficiaries.

At the same time, there is recognition that charity Boards need a mix of workers, door openers and fundraisers. It is, however, important that individuals understand what their role is. Involvement of a founder or major contributor can further complicate matters and trustees need to be alert to these nuances.

Purpose

A consistent understanding of the charity's purpose is vital for the Board of trustees as this will help to direct:

- what it does
- how it does it
- how it knows if it is being successful.

Purpose, with corresponding reporting on impact, are gaining momentum in the charity sector. More charities are reporting on how the money was spent and what it achieved rather than simply where it went. There is greater thought going into purpose and impact and how these are being communicated.

Impact can help with key decisions. For example, in social care, there may be instances when a decision needs to be taken between helping a large number of people a small amount or a lesser number but making a real difference. However, it is not just about quantity versus quality but also the broader impact. A charity's employees also need to understand its impact as it is difficult to tell a coherent story externally unless this is being measured internally.

A case study (Street League) was used to illustrate this further. This charity supports young people in regions of deprivation into education, training and employment. Making use of technology, they have developed a regularly updated 'impact dashboard' website that shows the young people's starting point, what barriers they report, where they progress to and whether they are still there after a period of time, with filters allowing the user to follow different stories. To enable this, data had to be collected in a structured way and initially this required a culture shift, persuading front line staff to collate this information which took away some of their time from delivering services.

However, the benefits have been significant in terms of presenting the charity's impact story and it has been used very successfully both internally but also with donors and for other external uses. There is an added advantage with there being only a single source of the truth rather than multiple reporting. Going forward, charities in similar sectors may be able to work together to collect the data for 'live' dashboards that would work for all. Charities may find themselves increasingly out of date if they do not focus on impact now.

Delivery of purpose

Effective delivery of purpose is dependent on making best use of the charity's resources. It also requires an awareness of change as what worked previously may no longer be appropriate.

Charities should consider a 'risk-assessed' reserves policy and should also ensure that their management information will highlight warning signs of developing issues before the charity ends up fighting for its survival. Commercial NEDs on trustee Boards may need to help their lay colleagues in this area.

There is often a gulf between common practice around risk registers in the commercial world and what exists in this space for a charity. However, it was agreed that the risk management thought process is the fundamental element, rather than necessarily how this is presented if insufficient resource exists for this. Clearly, good risk management needs the charity's strategy (purpose and impact) to be set up front in order to be able to identify the risks to achieving this. It also needs to be a 'live' tool for decision making purposes rather than a check box governance process.

Mergers

There is undoubtedly a need for more collaboration and potentially some consolidation within the sector. There are in excess of 200,000 charities in the UK and many operate in a similar space. As more are failing, Boards should give consideration to the possibility of a merger.

Traditionally, the charity sector has tended to view mergers negatively. However, viewing other charities as 'competition' may not be the right mindset and the merger that resulted in Cancer Research UK was a huge success. The Royal National Institute of Blind People (RNIB) recently identified that there are c.700 charities focused on the blind. 'Vision 2020' The right to sight' has been produced as a response. As a result, some charities have merged and others are more actively collaborating.

The question of whether or not to merge to achieve greater impact should be regularly revisited. There may also be triggers that allow for reconsideration of this such as the CEO's departure or loss of a major income stream.

Hallmarks of a successful charity

The workshop concluded with a brief look at the hallmarks of a successful charity, many of which had been touched on during the discussions:

- clarity of strategy
- operational efficiency
- risk management, reserves management and investment policy
- governance and management
- demonstrating social impact
- accurate management information and reporting
- competitive landscape/fragmenting market
- income generation/fundraising
- increased scrutiny.

The first three of these are internal choices, the middle three essential enablers and the final three external influences. A publication was provided which expanded on these in more detail.

Over 200,000
charities in the UK

Executive remuneration

Executive remuneration remains a matter of considerable focus for politicians, the media and the general public. There is a public perception of lack of fairness and real political impetus to respond to this. Arguably, executive remuneration has become a signature issue in relation to the erosion of public trust in big business.

The Government has been considering reforms to the governance of executive pay in an attempt to restore trust in this area and the revised UK Corporate Governance Code was issued around the time of the workshops.

The workshops provided the opportunity to discuss a number of issues relating to executive remuneration including 2018 pay trends, an update on the 2018 AGM season, global pay levels and structures and the newly issued UK Corporate Governance Code amendments.

PwC experts:

Phillippa O'Connor
phillippa.o.connor@pwc.com

Marcus Peaker
marcus.peaker@pwc.com

Einar Lindh
einar.lindh@pwc.com

Need to know

- Total remuneration outcomes have been broadly flat with continued restraint in awarding salary increases.
- ISS and shareholders are prepared to recommend and vote 'against' where salary increases are high, pay is not aligned to performance or disclosure is poor.
- New remuneration policies generally seek to adopt best practice.
- There is some evidence that UK shareholders may be more open to non-traditional schemes.
- New UK Corporate Governance Code recommendations around pay structure, disclosure, expansion of the Remuneration Committee remit and listening to the employee voice will come into force in 2019.

Pay trends

The workshop began with a look at 2018 pay trends. Although the data presented was for the FTSE 100, the trends were similar within the FTSE 250.

On a median basis, this season's FTSE 100 CEO single figure outcomes appear broadly stable versus the prior year but this conceals some nuance as follows:

- There have been average reductions of 17% for the highest paid CEOs (£10m plus) but overall the upper quartile of total pay is up 13%.
- The median single figure is down 14% on average for longer serving CEOs.
- 61% of CEOs have seen an increase over 2016.

Bonus and LTIP median and lower quartile outcomes increased slightly but the upper quartile decreased, resulting in narrower ranges.

Although there was a slight drop in salary freezes, there was low salary growth overall. Where an increase was given, it was often 2-3% and therefore generally in line with the broader workforce. This continued restraint is expected to persist going forward. Increases for CFOs have been slightly easier but even here the mood of restraint has prevailed.

Maximum LTIP opportunities were broadly similar to the prior year, although slightly down for CEOs and slightly up for CFOs. The CEO median LTIP opportunity reduced from 288% to 270% of salary, either due to companies reducing opportunity or making structural changes to the package.

Shareholders have not been sympathetic to companies with a large US presence claiming a need for higher salaries. Even a move from the FTSE 250 to the FTSE 100 has not generally been seen as grounds for an increase.

In summary, the past year was one where companies tended to keep their heads below the parapet. For most companies it was not a policy year and therefore there has been very little change.

2018 AGM season update

There is evidence of investors taking a harder line in FTSE 100 remuneration report voting outcomes. Although the median vote for is 96%, there has been more voting against. This has been for the usual reasons of:

- aggressive pay increases
- pay not aligned to performance
- poor disclosure.

A tougher stance by ISS may be part of the explanation for the lower voting outcomes as 'against' recommendations have been made at more than twice the rate of 2017. However, it is also worth noting that 'unqualified for' recommendations have also increased so the band of 'qualified for' recommendations has become narrower. Recent research by PwC suggests that ISS voting recommendations cause a 15-20% swing in the 'tail' of the voting register but have less impact on the top 10 investors.

There were limited 'red tops' from the Investment Association (IA), with only a slight increase, but a significant increase in amber tops with a broader range of language being used from 'members will note that…' to 'shareholders may be concerned that…'. The correlation between IA 'red tops' and ISS vote againsts is not perfect (c 60-70%).

PwC has long been advocating the need for proxy agencies to give more indication of what they will recommend. The new UK Corporate Governance Code encourages greater engagement by investors and proxy holders and it is hoped that the revised Stewardship Code will take this further.

Companies who receive more than a 20% vote against are now listed on an IA register but the large number of companies recorded on this diminishes the impact. PwC's view is that the mechanism would work better if it were for repeat offenders rather than one-off circumstances.

Proxy agencies sometimes take a different view in the US versus the UK, partly because of differing stringency in the voting but also because in the US the shareholders are mainly US based. There is also not the same culture of shareholder engagement and so ISS and Glass Lewis tend to have more power.

It is, however, worth noting that there is no real correlation between voting outcomes and buying/selling of shares, potentially mirroring the segregation in shareholders between their governance and investing arms.

A couple of case studies were discussed which illustrated that:

- quantum is still the overriding factor in executive pay and it often comes down to a view of 'how much is too much?'
- it is possible to get alternative pay models over the line provided there is a very clear strategic rationale and an appropriate amount of time is invested in consultation.

Global pay levels and structures

A graph illustrated that the US pays the highest total compensation, including pensions, followed by the UK and then Europe. Higher pay is correlated with higher market capitalisation.

US pay is more leveraged than the other markets, with the greatest opportunity from long term incentives and bonuses.

Performance share plans (PSPs) are dominant in the UK and becoming the norm in Europe whilst the US has a more equal split between PSPs and RSPs, with limited use of options.

The difference between the US and the UK in terms of quantum and make-up is likely to remain due to different market pressures, although the UK may get to a position of 20% RSPs over time. As noted earlier, the argument of needing to pay more due to US operations holds little sway among UK investors and there is not much international traffic of CEOs, despite claims they may go elsewhere.

Corporate Governance Code update

There have been some specific changes in the new UK Corporate Governance Code that will have implications for the Remuneration Committee in terms of:

- structure of pay
- disclosure
- expansion of remit
- listening to employee/stakeholder voice.

Structure

The structure points are more about doing what is right for the company and its strategy in terms of executive remuneration and the key changes in this area are:

- minimum of five year period from grant to realisation of LTIPs
- discretion in policies and plans to override formulaic outcomes
- Remuneration Committee Chair to have minimum of 12 months experience of (any) Remuneration Committee.

69% of FTSE 100 companies already have five year LTIPs so this change will not be significant. There is general encouragement for shares to be held for longer with some investors also wanting shares to be held for a lengthy period post cessation.

Whilst discretion is viewed as a helpful tool, there is some concern that it may be difficult to apply in practice. However, some companies have already used upwards and downwards discretion successfully over a period of time. Discretion aims to look at how targets were met, (e.g. riding a share price increase rather than being due to CEO performance), as opposed to purely whether they were met. There is an encouragement to Remuneration Committees not to hide behind arithmetic outcomes.

Disclosure

The key changes here are:

- wider workforce disclosure
- strategic rationale
- remuneration justification
- implementation of policy
- impact of Board discretion on remuneration outcomes.

In a change from the draft of the Code issued for consultation, wider workforce policies are now a Board issue – in terms of strategy and the impact of decisions, etc. – with the Remuneration Committee only focusing on the pay element, including any sales incentives.

Remit

The Remuneration Committee remit has now been formally extended to the Executive Committee which most are already covering in any case.

There is currently no intention to introduce further ratios at the Executive Committee level for fear that this may create another executive pay 'arms race.'

Employee voice

Three possible methods have been set out in the Code for engaging with employees:

- designated NED
- employee director
- formal stakeholder panel.

The FRC have also indicated that a combination of these can be used or indeed something else in addition or instead. The important aspect is that this needs to be a two-way dialogue which may be challenging in an international group. An annual survey is not enough as there should be evidence of engagement, how matters were taken into account in terms of executive pay and reporting back.

270% ***of salary = CEO median LTIP v 288% in prior year***

69% ***of FTSE 100 companies already have five year LTIPs***

Audit committee update

The Audit Committee Network holds technical workshops three times a year which cover an accounting update, a corporate governance and reporting briefing and also feature a couple of guest topics relevant to the Audit Committee agenda.

At the most recent workshops, the topics covered were:

- ***Accounting update – IFRS 9, IFRS 15 and IFRS 16***
- ***Corporate reporting/governance developments centred on the stakeholder agenda and the FRC's review and update of the UK Corporate Governance Code***
- ***The Task Force on Climate-related Financial Disclosures***
- ***The future of the audit profession.***

Accounting update

Impact of new standards

Our accounting update began with an overview of the Financial Reporting Council's (FRC) thematic reviews where it has announced it will be monitoring:

- the actual effect of adopting IFRSs 9 and 15 in 2018 interim accounts; and
- the expected effect of IFRS 16 in 2018 annual reports.

IAS 34 requires disclosure of the nature and effect of accounting policy changes. The FRC expects:

- quantitative disclosure – company-specific information and detailed explanations
- key judgements that are clearly explained
- explanation of how transition has been implemented.

Attendees were then taken through some findings relating to the implementation of IFRS 9, IFRS 15 and IFRS 16.

Observations – IFRS 9 Financial Instruments

To date we expect companies to have disclosed the effects of IFRS 9, IFRS 15 and IFRS 16 in their final accounts before implementation of the new requirements.

As part of a PwC review, we inspected the financial statements of 73 public companies (excluding financial institutions and telecom companies) with year ends in December 2017 and through to March 2018. We found that:

4	only referred to IFRS 9/no conclusion on impact of adoption
40	reported no material impact
1	did not mention IFRS 9
1	reported material impact and gave more information on adoption
27	reported no material impact and gave more information on adoption

Looking ahead, we would expect companies to report on:

Impairment – expected credit loss ('ECL')

- We would expect all companies with trade receivables to be impacted.
- No company mentioned that ECL had a material impact, with 63% explicitly saying the impact would be immaterial.

Hedging

- IFRS 9 was intended to broaden the opportunities for hedging, however no companies indicated any change in approach.

Modification of financial liabilities

- If financial liabilities have been modified in the past, we would expect an adjustment on transition to IFRS 9. No company mentioned this.

Accounting

Andrea Allocco
a.allocco@pwc.com

Peter Hogarth
peter.hogarth@pwc.com

Iain Selfridge
iain.selfridge@pwc.com

Jessica Taurae
jessica.taurae@pwc.com

Dave Walters
dave.walters@pwc.com

Corporate reporting/ governance

Mark O'Sullivan
mark.j.osullivan@pwc.com

John Patterson
john.t.patterson@pwc.com

Future of the audit profession

Hemione Hudson
hemione.hudson@pwc.com

Gilly Lord
gillian.lord@pwc.com

Task Force on Climate-related Financial Disclosures (TCFD)

Jon Williams
jon.d.williams@pwc.com

Jonathan Grant
jonathan.grant@pwc.com

IFRS 15 Revenue from Contracts with Customers

Using the same review of the 73 companies, the analysis showed that:

1	only referred to IFRS 15
27	reported no material impact
4	reported material impact and gave more information on adoption
41	reported no material impact and gave more information on adoption

Looking ahead, we would expect companies to report on:

Long-term contracts

- Only four companies stated that IFRS 15 would have a material impact, mostly with respect to long term contracts.

Transition method

- Only 32% of companies provided details on the method of transition, split evenly between full retrospective and modified retrospective adoption.

Tax impacts

- No companies mentioned any potential tax impact on transition to IFRS 15, or indicated that this has been considered.
- Companies should consider whether there is any cash tax impact from the changes or any deferred tax to account for if accounting recognition will be different from tax recognition.

Overall, even if something does not have a material impact, we recommend companies provide narrative to explain how management has come to this decision.

IFRS 16 Leases

When looking at IFRS 16, our analysis found that:

16	only referred to IFRS 16
8	provided detail on impact with quantification
47	provided some detail on impact
2	did not disclose any information regarding IFRS 16

Attendees were then taken through an overview of IFRS 16 and the potential implications for business.

IFRS 16 Headlines

- ✓ IFRS 16 requires lessees to recognise nearly all leases on the balance sheet and is effective 1 January 2019.
- ✓ The standard provides additional (and different) criteria for identifying leases.
- ✓ There is more guidance on lease term and variable rent, and enhanced disclosure requirements compared to IAS 17.
- ✓ The lessee will also need to present interest expense (on lease liability) and the depreciation charge (on the 'right to use' asset) separately.
- ✓ There are exemptions for short term leases (less than 12 months) and leases of low value assets.
- ✓ Lessor accounting remains largely unchanged from IAS 17; however, lessors are expected to be affected due to the changed needs and behaviours from customers which will impact their business model and lease products.
- ✓ A lessee has to choose either a full retrospective approach or a modified retrospective approach to transition to the new standard. The selected approach has to be applied to the entire lease portfolio.
- ✓ The part of the lease payment that represents cash payments for the principal portion of the lease liability is presented as a cash flow resulting from financing activities.
- ✓ The part of the lease payment that represents the interest portion of the lease liability is presented either as an operating cash flow or a cash flow resulting from financing activities (in accordance with the entity's accounting policy regarding the presentation of interest payments).

Measurement of lease liability

The lease liability is a present value of the lease payments during the lease term and is measured by discounting using the interest rate implicit in the lease, if it can be readily determined. If it cannot be determined, the lessee can use its incremental borrowing rate.

Why does it matter?

IFRS 16 will have a significant impact on all companies but the greatest impact on debt and EBITDA is expected in industries such as retail, airlines and professional services. It not only represents a significant accounting change for leases but could also have an impact on:

- a company's systems and also changes to processes
- triggers of covenant breaches
- planned deals (debt, IPO, M&A) and how the financials will look
- KPIs and the resulting knock on effect on remuneration schemes
- lessee behaviours and the subsequent effects on lessors.

Questions to ask management

1. Do you know how many leases you currently have, or where the agreements are? If not, how will you identify them all? How are you going to manage all the data in a consistent fashion?
2. What are the key policy choices, judgments and estimates to be made upon transition?
3. How will KPIs be impacted? What will this mean for covenants, investor communications, remuneration arrangements, etc.?

Lease payments that should be included in the liability are:

Fixed payments	+	Variable lease payments	+	Residual value guarantees	+	Exercise price of a purchase option	+	Penalties for terminating
Including in-substance fixed payments, less lease incentive payments.		Only if they depend on index/rate Measured using index/rate as at commencement date.		Expected payments lessee has to make under guarantee.		If the lessee is reasonably certain to exercise the option.		If the lease term reflects the termination by the lessee.

Corporate reporting/governance update

Our corporate reporting/governance update focussed on an update around the main developments centred on the stakeholder agenda.

The session began with an update on the most recent developments to be aware of, including the new Companies Act reporting regulations:

New Companies Act reporting regulations from BEIS

Section 172 and stakeholder engagement

- Reporting which was promised in Green Paper – overlaps with Code for relevant companies.
- Reporting on how section 172 is implemented. Should be reported in strategic report and on website.
- Stakeholder engagement reporting (split between employees and other stakeholders) should be included in the directors' report.
- Includes private companies and AIM companies – thresholds confirmed as 'large companies' under the Companies Act regime which consists of two of: (i) £36m turnover; (ii) £18m balance sheet assets; (iii) 250 employees; employee engagement: 250 employees only is sufficient.

Governance of private companies

- Reporting in the directors' report and on the company's website on how a chosen governance framework has been applied.
- Thresholds for mandatory reporting high – either (i) 2,000 employees or (ii) £200m turnover **and** £2bn balance sheet assets (all on a global basis).
- Applicable for subsidiaries.
- Set of principles that many companies will use is being developed by group chaired by James Wates, including the FRC, IoD, CBI, BVCA, IA and ICSA.
- All private companies encouraged to apply a governance framework.

Applicable date – *periods beginning on or after 1 January 2019*

In addition to this the expectations around corporate governance for companies registered on the AIM market have been increased:

- AIM Rule 26 has now changed to **require** website disclosure of 'details of a recognised corporate governance code that the Board of directors of the AIM company has decided to apply, how the AIM company complies with that code and, where it departs from its chosen corporate governance code, an explanation of the reasons for doing so'.
- Previously applying a code was voluntary.
- The Quoted Companies Alliance ('QCA') has issued a revised version of its code to take this change into account and is likely to be the framework that many AIM companies choose.
- Governance disclosures to be on website by 28 September 2018.

UK Corporate Governance Code

The Financial Reporting Council released the final version of the 2018 UK Corporate Governance Code after the Audit Committee Network sessions were complete but there was a discussion at the events of the proposals and the likelihood of any changes compared with the version consulted on.

A reminder of some of the more significant proposals and changes is set out below.

Structure

- The revised Code is intended to be 'shorter and sharper'- it has been reduced from 55 to 41 provisions.
- There have been changes to the structure of the Code: the main principle/supporting principle distinction has been removed.
- Some elements of the previous Code have been incorporated into the 'Revised Guidance on Board Effectiveness'.

Reporting

- There is a significant proposed shift in emphasis towards how a company has applied the principles to avoid 'boiler-plate' reporting.
- The Code consultation puts more emphasis on how a company should articulate action taken and resulting outcomes should be described.

It is important to report meaningfully when discussing the application of the Principles and to avoid boilerplate reporting. Instead, focus on how these have been applied, articulating what action has been taken and the resulting outcomes. Good practice examples of reporting will include signposting and cross-referencing to those parts of the annual report that describe how the Principles have been applied; this will help investors with their evaluation.

Independence of Non-Executive Directors

This is perhaps the area of change which provoked the most widespread debate and which was most commented on in the responses the FRC received to their consultation document.

Under the existing Code there is a list of indicators that a director may no longer be independent (including having been on the Board for nine years or more). If the Board decides that a director is still independent despite breaching one or more of these indicators, it needs to explain why in the annual report.

The FRC consulted on removing this ability for Boards to make their own judgements, so that being on the Board for nine years (for example) would automatically mean that a director could no longer be considered independent.

In the final version of the revised Code, Provision 10 has reverted to the existing basis (with some strengthening of the language around the criteria), so director independence remains a Board judgement.

Independence and tenure of Chairs

Under the existing Code the Chair of the Board is expected to be independent at the time of their appointment but loses this independence immediately after appointment because of the nature of the role.

The FRC consulted on extending the same independence framework to the Chair as for other directors. In response, many Chairs made it clear that they do not believe it to be possible to carry out their role fully while remaining 'independent' in any meaningful sense.

In the final version of the revised Code the FRC has reverted to the existing Code position on the Chair's independence BUT has also introduced a new Provision on tenure stating that: 'The chair should not remain in post beyond nine years from the date of their first appointment to the board. To facilitate effective succession planning and the development of a diverse board, this period can be extended for a limited time, particularly in those cases where the chair was an existing non-executive director on appointment. A clear explanation should be provided.' [Provision 19].

Board composition

Under the existing Code at least half the Board, excluding the Chair, should be independent directors. For companies outside the FTSE 350, only two independent directors are required.

The FRC consulted on amending the composition calculation to a majority of the Board, including the Chair, being independent – consistent with their proposals to include the Chair as an independent director.

Because of the outcome on Chair independence, the composition test has reverted in the final Code to at least half the Board excluding the Chair BUT the relaxation to allow only two independent directors on Boards outside the FTSE 350 has not been reinstated.

Committee composition

Consistent with the final position on Chair independence, the final version of the Code also allows companies outside the FTSE 350 to have only two independent directors on the Audit Committee. However, in a change from the existing Code, the Chair of the Board cannot be on the Audit Committee.

There is no change to the existing Code in relation to Remuneration and Nomination Committee composition (though the proposal which the FRC consulted on for a Remuneration Committee Chair to have at least twelve months experience on a Remuneration Committee before being appointed has been retained).

Workforce and other stakeholder engagement

Reporting on how the Board has engaged with a company's stakeholders is included in the final version of the Code, in a way that is broadly consistent with the new Companies Act reporting regulations discussed above (except that the Code refers to 'the workforce' as opposed to being restricted to UK employees).

The three mechanisms suggested by the Government for workforce engagement (a director appointed from the workforce; a formal workforce advisory panel; or a designated Non-Executive Director) have been retained, but it is now clearer that one of these methods or a combination of them can be used, and that other mechanisms are also possible (subject to being explained).

Remuneration

The major concern during the consultation process was that the scope of the Remuneration Committee was being expanded beyond a non-executive role.

This has been addressed in the final version of the Code, which clarifies that 'oversight of workforce policies and practices' is a whole Board responsibility (this has also been moved to the first section of the Code on Board leadership and purpose).

A number of other amendments have been made to the remuneration section of the Code since the consultation, reflecting the continuing focus on issues such as the use of discretion and the reputational risks associated with 'excessive pay'. It is probably the most heavily re-drafted area, without being fundamentally different.

The proposals relating to 'significant dissent' against AGM resolutions (which of course often relates to remuneration) have been retained broadly unchanged in the final version of the Code. 'Significant dissent' has been defined as 20% or more voting against (consistent with the Investment Association's public register), and new reporting on views received from shareholders and actions taken will be needed within six months of the vote.

Other amendments

Other aspects of the final Code which may attract commentary include:

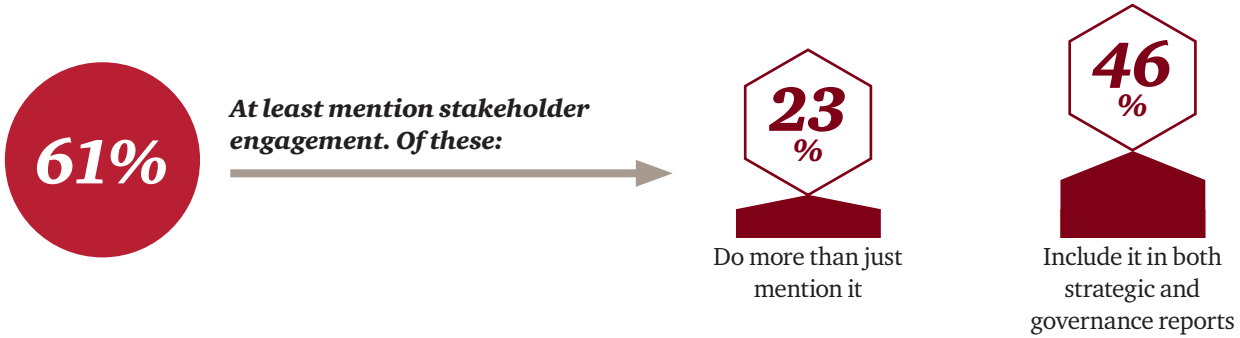
- The extension of annual re-election of all directors to companies outside the FTSE 350 (though externally facilitated Board evaluations have not been extended outside the FTSE 350 in the same way)
- A new focus on avoiding 'overboarding' of Non-Executive Directors and Chairs in Provision 15 in particular

Insight

Our view is that the majority of the changes to the FRC's original proposals are helpful and that the drafting is much clearer in a number of areas.

Initial observations on 2017 reporting season – main trends

The session then continued with a look at the findings from the PwC Corporate Reporting team's analysis of the 2017 reporting season. Not surprisingly, the team found some significant recognition of the stakeholder agenda:



+7% increase from the prior year in ***CSR linkage with strategy***

+11% increase from the prior year in ***Business Model linkage with strategy***

10% refer to section 172

14% explicitly mention the non-financial reporting regulations

The team had also noted a continuing trend towards including more forward-looking information, with more clarity on time horizons when discussing strategy and 35% of disclosures about the markets companies operate in including forward looking information.

Finally, looking to the medium term, an initial briefing was provided on preparations for the European Single Electronic Format ('ESEF'), which will require 'tagging' of financial statements and the whole of the annual report to be filed in a particular electronic format by 2020. The Financial Conduct Authority is leading the UK implementation of the EU requirement and may well go further than the EU is mandating. An update will be provided as more becomes known but, for now, the emphasis was on how there could be technological challenges with filing annual reports with the rich content of charts and diagrams that many currently include. It is hoped that the benefits of being able to compare financial data across companies and markets is balanced in the final implementation with the need for reports to remain easily useable by readers.

Task force on Climate-related Financial Disclosures (TCFD)

The next session focussed on the Task force on Climate-related Financial Disclosures (TCFD) which was set up by the G20 Financial Stability Board at the Paris Climate Summit in 2015. This aims to address concerns around insufficient disclosure of climate related risks to, and opportunities for, businesses. With 32 members drawn from a range of sectors and countries, including PwC Partner Jon Williams, the TCFD published its recommendations for voluntary, consistent climate-related financial disclosures in June 2017.

PwC's *'Low Carbon Economy Index 2017'* shows that the low carbon transition is already underway: global carbon intensity has fallen by an average of 1.4% each year since 2000. This is due to an improvement in energy efficiency, increasing renewables and a structural shift to lower carbon sectors such as services. This is happening in some countries faster than others, and the UK is leading the G20 countries with an annual decarbonisation rate of 4% since 2000. However, the current rates of decarbonisation around the world fall far short of the 6.5% annual rate needed to limit warming to two degrees. So companies should assess how climate change could impact their business and disclose activities and intended actions against the TCFD recommendations to help demonstrate to investors and other stakeholders that climate change risks are being considered.

The core disclosures

A. Governance
Disclose the extent of Board and management's oversight of climate-related risks and opportunities.

B. Strategy
Disclose the actual and potential impacts of climate-related risks and opportunities on the organisation's businesses, strategy, and financial planning where such information is material.

C. Risk management
Disclose how the organisation identifies, assesses, and manages climate-related risks.

D. Metrics and targets
Disclose the metrics and targets used to assess and manage relevant climate-related risks and opportunities where such information is material.

The PwC Sustainability team have put together some key questions to ask management against each disclosure.

Governance

1. Do Board members have a clear picture of the company's exposure to climate risks *beyond physical impacts?*
2. Does the Board have access to current and relevant climate expertise?
3. Are the right governance structures in place to manage climate risks and capture opportunities?
4. Is the Audit Committee sufficiently informed on the strategic, business and financial implications of climate change?
5. Is the Audit Committee satisfied that the financial statements appropriately reflect material climate risks?

Strategy

1. Have you conducted a strategic review of how climate change could impact the business (and its funded pension schemes)?
2. Does the executive team have an understanding of the potential impacts of future scenarios, including a 2°C world, on its business model in the next 3, 5, or 10 years?
3. Does the company's strategy today incorporate the implications of such scenario analysis?
4. Have you considered the opportunities presented by climate adaption and mitigation activities to your business model in different geographies?

Risk management

1. Do you have a clear picture of your company's exposure to climate risk?
2. Are there processes for prioritising climate risks and determining their relative materiality?
3. Do you have effective risk management processes in place that integrate climate change into enterprise risk management frameworks?
4. Does your risk or investment committee have adequate oversight of climate risks?
5. Are you able to explain these risks, and your management of them, to investors and regulators?

Metrics and Targets

1. Have you got the right data and systems in place to capture all the information needed to disclose?
2. Are you confident that the data you are disclosing is complete and accurate and a true reflection of your business?
3. Would your systems and data hold up under scrutiny by an investor or other key interested stakeholder?
4. Are you comfortable that your baseline targets are correct and an accurate measure on which to base future performance?
5. Have you identified metrics and targets that are genuinely material to your business and meaningful for your investors?

Considerations for business leaders

Investors' expectations are rising around the risks and opportunities that climate change brings. A major challenge for investors is the lack of good quality climate disclosures that are useful for them to base their investment decisions on. In fact, at launch, 237 companies publicly committed to support the TCFD. This includes over 150 financial institutions with assets of $82trn. Prominent investors have made climate change a top engagement priority and are using their voting power to get investees to disclose against the TCFD. PwC has helped a number of companies by providing a gap analysis on how they compare to their peers in terms of climate related issue management, transition risk analysis and TCFD implementation progress.

What actions should you be taking to generate value for your business?

- Understand how climate change could impact your business.
- Understand the materiality of any climate risks and opportunities.
- Quantitatively assess these risks and opportunities and prioritise accordingly.
- Be in a position to evaluate the implications of future climate scenarios on your strategy and business performance.
- Establish a governance process that will best position your business to manage material risks and capture the opportunities.
- Address stakeholder concerns around the resiliency of your business to climate change.

The future of the audit profession

Finally, there was some discussion around the current scrutiny of the audit profession and its future, as well as the role of the Audit Committee.

A number of points were made by attendees and this is an area which will continue to be debated. We would therefore welcome any views from the NED community on the matter.

180727-105044-LS-OS